

2009 RAPPORT ANNUEL
**DE L'OBSERVATOIRE
DE LA SÉCURITÉ
DES CARTES DE PAIEMENT**



31, rue Croix-des-Petits-Champs – 75049 Paris Cedex 01
Code Courrier : 11-2324

Rapport annuel 2009
de l'Observatoire de la sécurité des cartes de paiement

adressé à

Madame le Ministre de l'Économie, de l'Industrie et de l'Emploi
Monsieur le Président du Sénat
Monsieur le Président de l'Assemblée nationale

par

Monsieur Christian Noyer,

Gouverneur de la Banque de France,
Président de l'Observatoire de la sécurité des cartes de paiement

SOMMAIRE

AVANT-PROPOS	7
1 LES MESURES DE SÉCURITÉ PCI SONT-ELLES ADAPTÉES AU MARCHÉ FRANÇAIS ?	9
Description des mesures PCI	9
L'adéquation des mesures PCI au marché français	11
Conclusion	14
2 STATISTIQUES DE FRAUDE POUR 2009	17
Vue d'ensemble	17
Répartition de la fraude par type de carte	19
Répartition de la fraude par zone géographique	19
Répartition de la fraude par type de transaction	20
Répartition de la fraude selon son origine	23
3 VEILLE TECHNOLOGIQUE	27
Suivi de la mise en œuvre des solutions de paiement sans contact (par carte et mobile)	27
Sécurité du paiement à distance par courrier et téléphone	34
Sécurité des nouveaux terminaux de paiement « légers »	38
État d'avancement de la migration EMV	41
4 PERCEPTION PAR LES PORTEURS DE LA SÉCURITÉ DES CARTES DE PAIEMENT	45
Les résultats de l'étude sur la perception de la sécurité des cartes de paiement par les porteurs confirment les tendances observées en 2007	45
Les utilisateurs des paiements en ligne présentent une sensibilité réelle au risque de fraude et accueillent de manière favorable l'implication de leur banque dans la diffusion de dispositifs de sécurisation	48
Les réactions face à l'utilisation de dispositifs de sécurisation des paiements en ligne sont toujours positives	51
PROTECTION DU TITULAIRE D'UNE CARTE EN CAS DE PAIEMENT NON AUTORISÉ	59
MISSIONS ET ORGANISATION DE L'OBSERVATOIRE	63
LISTE NOMINATIVE DES MEMBRES DE L'OBSERVATOIRE	67
DOSSIER STATISTIQUE	69
DÉFINITION ET TYPOLOGIE DE LA FRAUDE RELATIVE AUX CARTES DE PAIEMENT	73

AVANT-PROPOS

L'Observatoire de la sécurité des cartes de paiement a été créé par la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne¹. Ses missions en font une instance destinée à favoriser l'échange d'informations et la concertation entre toutes les parties concernées (consommateurs, commerçants, émetteurs et autorités publiques) par le bon fonctionnement et la sécurité des systèmes de paiement par carte².

Conformément à l'alinéa 6 de l'article L. 141-4 du Code monétaire et financier, le présent rapport constitue le rapport d'activité de l'Observatoire qui est remis au ministre chargé de l'économie et des finances et transmis au Parlement. Il comprend une étude sur les mesures de sécurité PCI et leur adaptation au marché français (1^{ère} partie), puis une présentation des statistiques de fraude pour 2009 (2^{ème} partie) et une synthèse des travaux conduits en matière de veille technologique (3^{ème} partie). Enfin, le rapport comprend une étude portant sur la perception par les porteurs de la sécurité des cartes de paiement (4^{ème} partie).

¹ Les dispositions légales relatives à l'Observatoire figurent à l'article L. 141-4 du Code monétaire et financier.

² Pour ses travaux, l'Observatoire distingue les systèmes de paiement par carte de type « interbancaire » et ceux de type « privé ». Les premiers correspondent à ceux dans lesquels il existe un nombre élevé d'établissements de crédit émetteurs et acquéreurs. Les seconds correspondent à ceux dans lesquels il existe un nombre réduit d'établissements de crédit émetteurs et acquéreurs.

1 | LES MESURES DE SÉCURITÉ PCI SONT-ELLES ADAPTÉES AU MARCHÉ FRANÇAIS ?

Au titre de sa mission de suivi des politiques de sécurité mises en œuvre par les émetteurs et les accepteurs, l'Observatoire a souhaité, en 2010, évaluer si les mesures dites « PCI », communes aux réseaux internationaux de carte, et qui spécifient les dispositions de sécurité pour le stockage et l'utilisation des données de cartes³, étaient adaptées au marché français, et ainsi identifier les éventuelles difficultés qui pourraient freiner l'application de ces exigences en France. Il s'agissait notamment d'examiner, pour les opérations effectuées en France, si les mesures PCI couvraient de manière appropriée les besoins de protection des différentes données sensibles des cartes et si les charges de contrôle imposées aux différents acteurs étaient adaptées aux risques rencontrés.

Les mesures PCI s'appliquent à l'ensemble des acteurs de la chaîne d'acceptation et d'acquisition, c'est à dire aux commerçants, aux banques acquéreurs et aux prestataires de service des uns et des autres.

L'Observatoire a conduit son étude sur la base d'informations recueillies auprès de représentants des établissements émetteurs, des commerçants, des systèmes de cartes ainsi que de prestataires techniques impliqués dans la chaîne de personnalisation ou la gestion des équipements⁴.

1|1 Description des mesures PCI

Les mesures dites PCI sont développées par l'organisme « PCI SSC » (Payment Card Industry Security Standard Council), créé par American Express, Discover Financial Services, JCB International, MasterCard Worldwide et Visa Inc. International. Elles s'appliquent de manière mondiale à l'ensemble des acteurs de la filière d'acceptation et d'acquisition (banques acquéreurs, commerçants, prestataires de service exploitant des plates-formes de paiement, etc.) participant aux systèmes de paiement par carte membres de PCI, à la fois pour les transactions transfrontalières, mais aussi pour les transactions domestiques dans le cas de cartes co-badgées avec un système national⁵. Compte tenu de ce champ d'application, ces mesures prennent, de fait, largement le caractère de standards.

Les mesures PCI visent à lutter contre le détournement des données de carte afin d'éviter leur réutilisation frauduleuse.

Plusieurs séries de mesures de sécurité ont été édictées par PCI SSC, parmi lesquelles on retiendra principalement pour les besoins de cette étude les mesures appelées « PCI DSS » (PCI Data Security Standard), qui visent à protéger les données transmises au travers des

³ Numéro, date d'expiration, CVx2, code confidentiel.

⁴ BPCE, Société Générale, La Banque Postale, S2P, Visa Europe France (ex-SAS Carte Bleue), Mastercard, American Express, Concert International, Lafon, Atos Worldline, Lyra Network, ainsi que, de façon groupée, les entreprises membres de MERCATEL, de la FCD, de la FEVAD, de la Fédération des Enseignes du Commerce Associé, de l'U.C.A, de la FPS et des fédérations membres du Conseil du Commerce de France (48 enseignes commerciales ayant participé à cette réponse).

⁵ C'est notamment le cas des cartes émises en France par les membres du Groupement des Cartes Bancaires « CB ».

systèmes d'information de la chaîne d'acquisition du paiement par carte, ou stockées dans ces systèmes (voir Encadré 1)⁶ :

Encadré 1 – Présentation des mesures PCI DSS

PCI DSS se compose de 12 types de mesures, réparties en 6 thèmes :

Création et gestion d'un réseau sécurisé

1. Installer et gérer une configuration de pare-feu pour protéger les données des titulaires de cartes
2. Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur

Protection des données des titulaires de cartes

3. Protéger les données de cartes stockées
4. Crypter la transmission des données des titulaires de cartes sur les réseaux publics

Gestion d'un programme d'analyse des vulnérabilités

5. Utiliser des logiciels antivirus et les mettre à jour régulièrement
6. Développer et gérer des systèmes et des applications sécurisés

Mise en œuvre de mesures de contrôle d'accès strictes

7. Restreindre l'accès aux données des titulaires de cartes aux seules personnes qui doivent les connaître
8. Affecter un identifiant unique à chaque utilisateur d'ordinateur
9. Restreindre l'accès physique aux données des titulaires de cartes

Surveillance et test réguliers des réseaux

10. Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données des titulaires de cartes
11. Tester régulièrement les processus et les systèmes de sécurité

Gestion d'une politique de sécurité des informations

12. Gérer une politique de sécurité des informations

La vérification de la mise en œuvre de ces mesures donne lieu à une certification de conformité. Pour ce faire, des audits sont conduits par des organismes spécialisés accrédités par PCI SSC, auprès des commerçants et des prestataires techniques, selon différentes méthodes tenant compte du volume de transactions réalisées. Les modalités de ces audits et de la certification qui en résulte sont propres à chaque système de paiement par carte. A titre d'illustration, pour MasterCard Worldwide, elles se déclinent selon 4 niveaux en fonction de l'importance des acteurs concernés :

- niveau 1 : pour les acteurs gérant plus de 6 millions de transactions cartes par an (tous canaux de commerce confondus) ou ayant déjà subi une compromission, le programme prévoit que l'acteur concerné doit effectuer un audit annuel de sécurité sur site de son système d'information et une analyse trimestrielle des vulnérabilités de son réseau de télécommunication ;
- niveau 2 : les acteurs gérant entre 1 et 6 millions de transactions cartes par an sont tenus de répondre à un questionnaire annuel d'auto-évaluation et de réaliser une analyse trimestrielle des vulnérabilités réseaux ;
- niveau 3 : les acteurs gérant plus de 20 000 transactions cartes en commerce électronique et moins de 1 million de transactions cartes par an au total sont eux aussi tenus de

⁶ PCI SSC a également promulgué des normes visant à la protection des automates de vente (PCI UPT), des terminaux (PCI PED), ou des applications (PCI PA DSS).

répondre à un questionnaire annuel d'auto-évaluation et de réaliser une analyse trimestrielle des vulnérabilités réseaux ;

- niveau 4 : il est recommandé aux autres acteurs de répondre à un questionnaire annuel d'auto-évaluation établi par PCI SSC et de procéder à un test d'évaluation trimestriel des vulnérabilités du système d'information et du réseau de télécommunication.

1 | 2 L'adéquation des mesures PCI au marché français

La gouvernance de PCI SSC

Les acteurs impliqués

La composition des organes de gouvernance de PCI SSC, qui regroupent les 5 membres fondateurs, n'a pas évolué depuis la création de cet organisme en 2006. Si cela est de nature à faciliter le processus de décision, notamment lors des phases récurrentes d'évolution des standards, certains organismes interrogés par l'Observatoire ont souligné qu'une telle situation ne permettait pas la représentation des acteurs auxquels s'appliquent les normes. Selon ces organismes, une évolution de la gouvernance de PCI SSC est souhaitable. L'European Payments Council (EPC), structure de coordination bancaire au plan européen pour la mise en œuvre du projet SEPA (Espace unique de paiement en euros), étudie ainsi la possibilité d'être représentée au sein de PCI SSC. Plus généralement, il a été souligné l'importance que les structures de gouvernance actuelles soient plus proches des intérêts qu'elles sont chargées de protéger, sur un plan sectoriel ou géographique.

La mise en œuvre des mesures

Chacun des réseaux membres de PCI SSC a défini ses propres modalités d'application des mesures PCI. En particulier, les dates limites de mise en conformité ainsi que les modalités de calcul des seuils dans le processus de certification varient selon le système de paiement par carte considéré. La plupart des participants à l'enquête menée par l'Observatoire, acceptant ou traitant des cartes de différents systèmes, souligne ainsi un besoin d'harmonisation dans l'interprétation des mesures PCI, afin d'assurer une plus grande efficacité opérationnelle et une meilleure maîtrise des coûts.

Par ailleurs, les mesures PCI s'appliquent à un environnement technologique par nature évolutif. Ceci conduit PCI SSC à les réviser régulièrement de façon à tenir compte de l'état de l'art en matière de sécurité. Si les participants à l'enquête ne contestent pas la nécessaire évolution des mesures, ceux-ci jugent parfois trop élevée la fréquence de leur mise à jour, ce qui peut entraîner des difficultés lors de la mise en place de mesures correctrices.

L'application à l'environnement monétique français

Champ d'application des mesures PCI

Les mesures PCI DSS visent à protéger l'ensemble de la filière d'acceptation et d'acquisition. Elles couvrent ainsi de manière large les données figurant sur la carte, c'est-à-dire à la fois celles qui sont embossées et celles qui sont enregistrées sur la piste ou dans la puce. L'objectif poursuivi est en effet de lutter contre tout type de compromission, en tenant compte des différents types d'utilisation des données de la carte selon le canal de paiement utilisé.

Les représentants du commerce sont toutefois réservés sur la pertinence de l'application au marché français des mesures concernant la protection des données de la piste, faisant observer que les transactions réalisées en France reposent en très grande majorité sur la puce présente sur les cartes de paiement, qui bénéficient par là même de protections cryptographiques élevées. Toutefois, la protection des données associées (numéro de carte, date d'expiration) et des données embossées ou imprimées sur la carte (les mêmes que citées précédemment ainsi que le CVx2) est importante pour empêcher leur réutilisation frauduleuse notamment dans le cadre du e-commerce.

Les mêmes acteurs font en outre valoir que le fait de désensibiliser les données de carte contre tout risque de compromission leur permettrait de s'affranchir du respect des mesures PCI, que celles-ci concernent la protection des informations embossées sur la carte, inscrites sur la piste ou stockées dans la puce. Plus généralement, la question de la pertinence de la gestion de ces données sensibles par les commerçants reste posée, tout en notant que ceux-ci assurent la maîtrise de la sécurité de leurs systèmes.

Chevauchement des mesures PCI avec d'autres normes de sécurité

Certains participants à l'enquête ont fait valoir que les mesures PCI DSS apparaissent proches de normes de sécurité internationales, telles les normes ISO 27000⁷, ou de mesures applicables en France, telles les recommandations de la CNIL (voir Encadré 2), de sorte qu'elles pourraient être considérées comme faisant double emploi avec ce qui est mis en œuvre par les acteurs qui les appliquent. Un point de vue inverse a toutefois été défendu par d'autres participants qui ont souligné que la mise en œuvre des normes ISO 27000 ou des recommandations de la CNIL contribuait à assurer la conformité aux mesures PCI.

De manière générale, des remarques analogues ont été formulées quant au chevauchement, d'une part des mesures PCI DSS et PCI PED avec les principes de sécurité du standard de carte à puce EMV et, d'autre part, des mesures PCI UPT (PCI Unattended Payment Terminal, prescrivant des protections physiques et logiques des composants électroniques des terminaux) avec les mesures AFAS⁸ (destinées à lutter contre la capture de données de carte sur les Distributeurs Automatiques de Billets et les Distributeurs Automatiques de Carburant). Il convient cependant de noter que le champ des mesures PCI est plus large que celui de ces autres normes et que la combinaison de l'ensemble permet de couvrir les différents canaux de compromission de données tels qu'identifiés dans le cadre d'une analyse de risques.

⁷ Série de normes dédiées à la sécurité de l'information, définissant le cadre de mise en œuvre d'un système de gestion de la sécurité, d'un catalogue de mesures de sécurité et d'un processus de gestion du risque.

⁸ « Anti Fishing Anti Skimming », ensemble de mesures imposées par le Groupement des Cartes Bancaires « CB » en 2005 afin de protéger les automates de paiement et de retrait.

Encadré 2 – Les recommandations de la CNIL

Compte tenu des risques liés à la circulation du numéro de carte bancaire en cas de vente à distance, la Commission a adopté en 2003⁹ une recommandation reprenant, en les appliquant à ce domaine, les grands principes de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Elle a tout particulièrement mis l'accent sur les conditions de sécurité entourant la collecte et le traitement du numéro de carte bancaire.

La CNIL considère ainsi qu'aucune décision impliquant une appréciation sur un comportement humain ne saurait avoir pour seul fondement un traitement automatisé de données à caractère personnel. En principe, la durée de conservation du numéro de carte bancaire ne saurait excéder le délai nécessaire à la réalisation de la transaction pour laquelle il a été collecté. Si une conservation de ce numéro à d'autres fins est prévue, elle est subordonnée au recueil du consentement explicite de la personne concernée. La Commission a déjà mis en demeure plusieurs hôtels¹⁰ pour avoir conservé cette information sans avoir obtenu de consentement préalable. Enfin, les personnes doivent être informées de la mise en œuvre de ce traitement conformément aux dispositions de l'article 32 de la loi susvisée.

L'augmentation des achats sur Internet entraîne la mise en œuvre par les professionnels concernés de nouveaux traitements de données à caractère personnel notamment afin de lutter contre la fraude. Des outils de détection des comportements atypiques des porteurs de carte bancaire ou des techniques d'authentification complémentaire du porteur sont ainsi mises en place. Certains de ces dispositifs sont susceptibles d'exclure des personnes du bénéfice d'un droit ou d'un contrat en l'absence de toutes dispositions législatives et réglementaires le prévoyant en empêchant, même de manière temporaire, une personne d'utiliser sa carte de paiement. Ces traitements sont donc soumis à autorisation préalable de la Commission en application des dispositions de l'article 25.I.4° de la loi susvisée. Dans le cadre de l'examen de ces dossiers, la Commission vérifie notamment les conditions d'information des personnes et les conséquences attachées à la mise en œuvre de ces traitements.

La certification

Processus de certification

La certification de la conformité aux mesures PCI est effectuée par des prestataires (Qualified Security Assessors - « QSA ») accrédités par PCI SSC, et dont la liste est publiée par ses membres fondateurs. Les systèmes de paiement par carte peuvent également imposer une analyse trimestrielle des vulnérabilités, effectuée par des « ASV » (Approved Scanning Vendors), en fonction du nombre de transactions traitées chaque année. Les établissements acquéreurs sont quant à eux soumis aux normes PCI sans être formellement certifiés conformes par PCI SSC.

La publication de la liste des QSA/ASV et des résultats des audits de certification par chacun des systèmes de paiement par carte assure la transparence de ce processus. Les acteurs soumis aux mesures PCI disposent ainsi en temps réel d'une base leur permettant de s'assurer de la qualité des matériels dont ils sont équipés et de la conformité des prestataires auxquels ils délèguent certaines parties du processus d'acquisition.

De telles publications –ajouts et retraits des listes des acteurs certifiés– comportent toutefois un risque intrinsèque de dépendance de ces acteurs à l'égard des systèmes de paiement par carte seuls chargés de la mise en œuvre et de la gestion de ces listes. Leurs modifications peuvent en effet avoir des conséquences préjudiciables aux acteurs concernés, d'autant plus importantes qu'ils agissent dans le cadre d'un marché très concurrentiel.

⁹ <http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/13/>

¹⁰ <http://www.cnil.fr/en-savoir-plus/fiches-pratiques/fiche/article//du-bon-usage-des-donnees-bancaires-collectees-par-les-hotels/#>

La majorité des acteurs interrogés par l'Observatoire fait par ailleurs remarquer que la mise en œuvre des mesures PCI est lourde et complexe, et qu'il leur est ainsi nécessaire de faire appel à des sociétés de conseil pour y parvenir. Or, ils soulignent le conflit d'intérêt qui peut résulter du fait que ces sociétés sont aussi le plus souvent accréditées par PCI SSC pour réaliser les audits de conformité. Outre que ces sociétés disposent ainsi, par la conjonction de leurs deux missions, d'une position d'influence sur la mise en œuvre des mesures, elles peuvent également disposer à l'occasion de leur intervention d'une visibilité complète des sécurités mises en œuvre sur le système d'information de l'acteur. Dans ce contexte, certains acteurs ont émis le souhait que les services d'audit interne des entreprises soient le cas échéant mieux impliqués dans le processus de certification.

Mécanisme de sanctions

Toute non conformité est susceptible d'entraîner des sanctions de différentes natures, dont :

- la prise en charge des coûts éventuellement induits par la non conformité (opérations frauduleuses, réémission des cartes, etc.) ;
- des sanctions pécuniaires pour les banques acquéreurs, qui sont définies et perçues indépendamment par chaque réseau membre de PCI SSC en se référant au nombre de jours de non conformité ou au nombre de transactions réalisées ;
- la suspension du compte du commerçant.

Ces mécanismes de sanction, fondés sur la relation contractuelle encadrant l'acceptation des cartes d'un réseau, traduisent l'aspect coercitif des mesures PCI. Ils ne sont pas contestés par les acteurs interrogés dans le cadre de cette enquête, mais certains d'entre eux relèvent toutefois le caractère parfois élevé des sommes dues aux réseaux membres de PCI SSC, par ailleurs susceptibles de se cumuler au montant des transactions frauduleuses subies sur la période considérée.

1|3 Conclusion

Les réponses fournies dans le cadre de l'étude menée par l'Observatoire confirment la nécessité de mettre en œuvre des mesures de protection des données de carte dans l'ensemble du processus d'acceptation et d'acquisition. Les mesures PCI représentent dans ce cadre une bonne pratique, contribuant à élever le niveau de sécurité des processus et matériels utilisés. Leur adoption par les systèmes de paiement par carte internationaux, y compris pour les cartes nationales avec lesquelles ceux-ci ont des accords de co-badgeage, donne à ces mesures le caractère de standards de fait.

Leur adéquation au marché français n'est toutefois pas sans soulever de questions. La spécificité de l'utilisation des cartes à puce paraît à certains acteurs interrogés insuffisamment reconnue par PCI SSC. D'autres soulignent à l'inverse que les données de carte peuvent être gérées dans de nombreux environnements tout au long des phases d'acceptation et d'acquisition, et que la réutilisation frauduleuse de ces données constitue un risque majeur. Or les recommandations adoptées par la CNIL en la matière, de même que les études menées par l'Observatoire depuis sa création, confirment l'enjeu d'une telle protection. Dans ce contexte, la possibilité de désensibiliser les données de carte est également évoquée, les représentants des commerçants s'interrogeant sur la pertinence de la gestion de ces données aujourd'hui sensibles dans leurs environnements.

De plus, la question de la représentation des acteurs français ou européens au sein de PCI SSC a paru cruciale pour permettre une bonne adaptation des mesures PCI aux

spécificités locales. Il serait ainsi souhaitable que la gouvernance de cet organisme soit élargie, et que l'European Payments Council (EPC), qui travaille à l'interopérabilité des paiements par carte en Europe, puisse y siéger. Dans cette optique, des représentants des banques et du commerce appellent à la création d'un observatoire européen de la fraude, à l'image du dispositif mis en œuvre en France par l'Observatoire de la sécurité des cartes de paiement. Une telle instance permettrait notamment de répondre aux attentes des acteurs de la chaîne de paiement en donnant des orientations adaptées au marché européen.

En outre, les spécificités propres aux systèmes de paiement par carte membres de PCI SSC dans l'application des mesures PCI, ou dans la mise en œuvre du mécanisme d'évaluation de la conformité, sont susceptibles d'accroître la charge de mise en œuvre par les acteurs. Une meilleure concertation entre systèmes de paiement par carte devrait permettre d'y remédier.

Les acteurs interrogés ont également noté la lourdeur, jugée parfois excessive y compris en termes de coût, des procédures d'évaluation de la conformité, voire de sanction, imposées aux acteurs de la filière d'acceptation et d'acquisition. Il serait aussi important d'éviter toute position d'influence et tout conflit d'intérêt dont pourraient profiter les sociétés accréditées pour réaliser les audits de conformité des acteurs concernés. Des améliorations tangibles sont souhaitables sur ces points.

2 | STATISTIQUES DE FRAUDE POUR 2009

Depuis 2003, l'Observatoire établit des statistiques de fraude des cartes de paiement de type « interbancaire » et de type « privatif », sur la base de données recueillies auprès des émetteurs et des accepteurs. Ce recensement statistique suit une définition et une typologie harmonisées, établies dès la première année de fonctionnement de l'Observatoire et reprises en annexe E du présent rapport. Une synthèse des statistiques pour 2009 est présentée ci-après. Elle comporte une vue générale de l'évolution de la fraude, selon le type de carte (« interbancaire » ou « privatif »), le type de transaction effectué (transactions nationales ou internationales, transactions de proximité ou à distance, transactions de paiement ou retrait) et l'origine de la fraude (carte perdue ou volée, carte non parvenue, carte altérée ou contrefaite, numéro de carte usurpé). En complément, une série d'indicateurs détaillés est présentée dans l'annexe D de ce rapport.

Encadré 3 – Statistiques de fraude : les contributeurs

Afin d'assurer la qualité et la représentativité des statistiques de fraude, l'Observatoire recueille les données de l'ensemble des émetteurs de cartes, de type « interbancaire » ou « privatif ». Il complète ces données par des statistiques établies par la Fédération du e-commerce et de la vente à distance (Fevad), qui consulte un échantillon de 33 entreprises représentant 26 % du chiffre d'affaires de la vente à distance aux particuliers.

Les statistiques calculées par l'Observatoire portent ainsi sur :

- 429,4 milliards d'euros de transactions réalisées en France et à l'étranger à l'aide de 62,4 millions de cartes de type « interbancaire » émises en France (dont 1,54 million de porte-monnaie électroniques) ;
- 24,2 milliards d'euros de transactions réalisées (principalement en France) avec 28,2 millions de cartes de type « privatif » émises en France ;
- 23,7 milliards d'euros de transactions réalisées en France avec des cartes de paiement de types « interbancaire » et « privatif » étrangères.

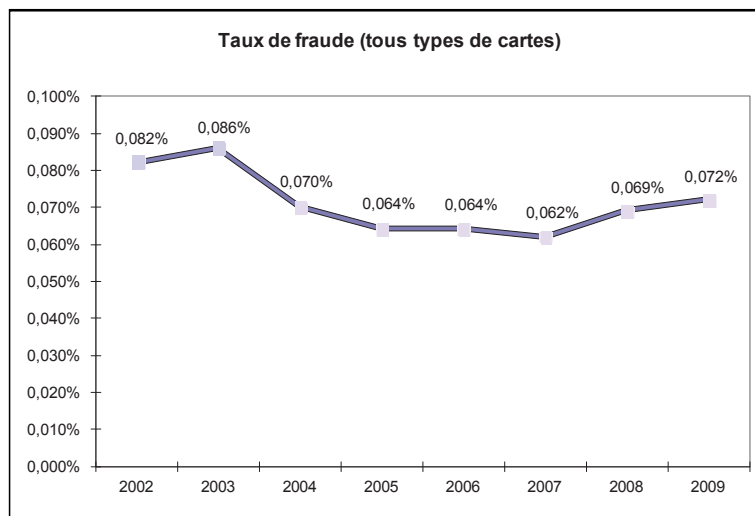
Les données recueillies proviennent :

- de dix émetteurs de cartes privées : American Express, Banque Accord, BNP Paribas Personal Finance, Cofidis, Cofinoga, Diners Club, Finaref, Franfinance, S2P et Sofinco ;
- des 136 membres du Groupement des Cartes Bancaires « CB ». Les données ont été obtenues par l'intermédiaire de ce dernier, ainsi que de MasterCard et de Visa Europe France ;
- des émetteurs du porte-monnaie électronique Moneo.

2|1 Vue d'ensemble

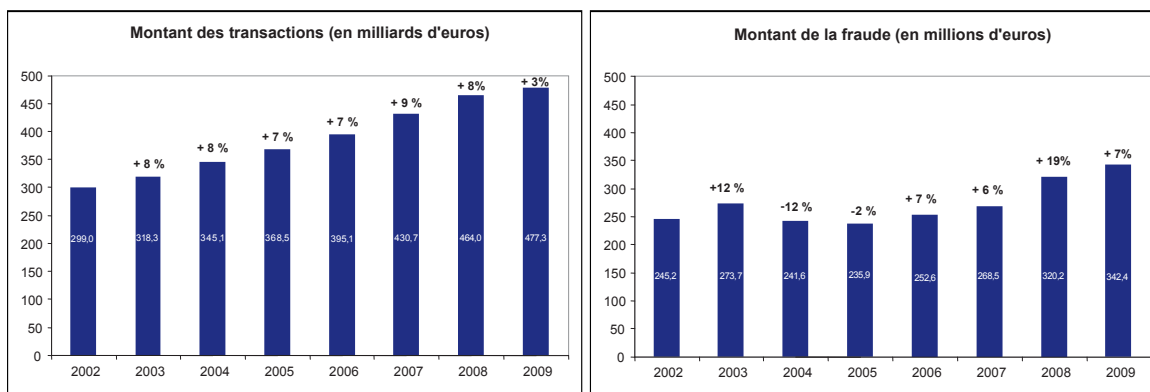
Le taux de fraude sur les paiements et les retraits par carte enregistré en 2009 dans les systèmes français est de 0,072 %. Il est en augmentation comparé à celui des années précédentes (0,069 % en 2008 et 0,062 % en 2007 – voir Tableau 1). En effet, la progression des montants de fraude (342,4 millions d'euros en 2009 contre 320,2 millions d'euros en 2008, soit une hausse de 6,9 %) est plus importante que la croissance du montant des transactions (477,3 milliards d'euros en 2009 contre 464,0 milliards d'euros en 2008, soit une hausse

de 2,9 % – voir Tableau 2). Le montant moyen d'une transaction frauduleuse est en légère hausse, à 136 euros contre 131 euros en 2008.



Source : Observatoire de la sécurité des cartes de paiement

▲ Tableau 1 – Évolution du taux de fraude pour tous types de cartes



Source : Observatoire de la sécurité des cartes de paiement

▲ Tableau 2 – Évolution des montants de transactions et de fraude

On observe une augmentation du taux de la fraude émetteur –c'est-à-dire de l'ensemble des paiements et retraits frauduleux réalisés en France et à l'étranger avec des cartes émises en France. Il s'établit en 2009 à 0,059 %, pour un montant de fraude de 265,6 millions d'euros (contre 0,057 % et 249,2 millions d'euros en 2008).

Le taux de la fraude acquéreur –c'est-à-dire de l'ensemble des paiements et retraits frauduleux réalisés en France quelle que soit l'origine géographique de la carte– est en légère augmentation. Il s'établit en 2009 à 0,048 %, pour un montant de fraude de 220,8 millions d'euros (contre 0,045 % en 2008, pour un montant de fraude de 201,9 millions d'euros).

L'annexe D du présent rapport regroupe des tableaux détaillés des volumes et valeurs de transaction et des volumes et valeurs de fraude, par type de carte, zone géographique, type de transaction et origine de fraude.

2|2 Répartition de la fraude par type de carte

Taux de fraude (Montant de la fraude en millions d'euros)					
	2005	2006	2007	2008	2009
Cartes de type « interbancaire »	0,064 % (218,8)	0,065 % (237,0)	0,063 % (253,6)	0,070 % (304,3)	0,072 % (324,3)
Cartes de type « privé »	0,067 % (17,1)	0,052 % (15,6)	0,052 % (15,0)	0,054 % (16,0)	0,068 % (18,2)
Total	0,064 % (235,9)	0,064 % (252,6)	0,062 % (268,5)	0,069 % (320,2)	0,072 % (342,4)

Source : Observatoire de la sécurité des cartes de paiement

▲ Tableau 3 – Répartition de la fraude par type de carte

Pour les cartes de type « interbancaire », le taux de fraude est en légère hausse en 2009, et s'établit à 0,072 %, pour un montant de fraude de 324,3 millions d'euros (contre 0,070 % en 2008, pour un montant de fraude de 304,3 millions d'euros). Pour ce type de carte, les taux de fraude émetteur et acquéreur sont respectivement de 0,059 % et de 0,048 % (contre 0,057 % et 0,046 % en 2008). La valeur moyenne d'une transaction frauduleuse est de 132 euros, contre 127 euros en 2008.

Pour les cartes de type « privé », le taux de fraude augmente sensiblement, à 0,068 %, pour un montant de fraude de 18,2 millions d'euros (contre 0,054 % et 16,0 millions d'euros en 2008). Pour ce type de cartes, les taux de fraude émetteur et acquéreur s'établissent respectivement à 0,053 % et à 0,059 % (contre 0,046 % et 0,042 % en 2008). La valeur moyenne d'une transaction frauduleuse s'élève à 324 euros en 2009, contre 357 euros en 2008.

2|3 Répartition de la fraude par zone géographique

Taux de fraude (Montant de la fraude en millions d'euros)					
	2005	2006	2007	2008	2009
Transactions nationales	0,029 % (97,8)	0,031 % (109,6)	0,029 % (114,5)	0,031 % (130,9)	0,033 % (144,0)
Transactions internationales	0,408 % (138,1)	0,362 % (143,0)	0,368 % (154,0)	0,427 % (189,4)	0,449 % (198,4)
Dont émetteur français et acquéreur étranger	0,458 % (64,1)	0,453 % (76,4)	0,476 % (85,3)	0,594 % (118,3)	0,594 % (121,6)
Dont émetteur étranger et acquéreur français	0,373 % (74,1)	0,295 % (66,5)	0,288 % (68,7)	0,291 % (71,0)	0,324 % (76,8)
Total	0,064 % (235,9)	0,064 % (252,6)	0,062 % (268,5)	0,069 % (320,2)	0,072 % (342,4)

Source : Observatoire de la sécurité des cartes de paiement

▲ Tableau 4 – Répartition de la fraude par zone géographique

La répartition de la fraude par zone géographique demeure marquée par un déséquilibre entre les transactions nationales et internationales : 58 % de la fraude portent sur les transactions internationales, alors que ce type de transaction compte à peine pour 9 % de la valeur des transactions par carte enregistrées dans les systèmes français.

Dans un contexte de croissance du montant des transactions nationales (+ 3,2 %), le taux de fraude de celles-ci est en légère hausse, mais demeure à un niveau très faible, à 0,033 % en 2009, contre 0,031 % en 2008.

La fraude sur les transactions internationales augmente pour sa part en 2009, à la fois en taux et en montant. Le taux de fraude liée aux transactions effectuées à l'étranger avec des cartes émises en France reste très élevé à 0,594 %, pour un montant de fraude de 121,6 millions d'euros (contre 118,3 millions d'euros en 2008). Le taux de fraude liée aux transactions effectuées en France avec des cartes émises à l'étranger est en hausse et s'établit à 0,324 %, pour un montant de fraude de 76,8 millions d'euros (contre 0,291 % en 2008, pour un montant de fraude de 71,0 millions d'euros).

Encadré 4 – Répartition du préjudice de la fraude

Depuis 2007, l'Observatoire estime, pour l'ensemble des systèmes de type « privatif » et de type « interbancaire », des indicateurs de la répartition du préjudice de la fraude entre le porteur, le commerçant et leurs banques. Il est important de noter que ces indicateurs ne valent que pour le préjudice lui-même, et non pour les coûts totaux de traitement ou d'assurance engendrés par la fraude. Ces indicateurs donnent une tendance mais restent théoriques et ne peuvent refléter que la répartition directe de la fraude supportée par les acteurs. Par construction en effet, ils se réfèrent aux dispositions légales et réglementaires encadrant l'opposition par le porteur en cas de perte ou de vol, ainsi que la contestation par celui-ci en cas d'utilisation frauduleuse de sa carte. De plus, ils ne peuvent tenir compte totalement des pratiques commerciales des émetteurs ou des acquéreurs.

Tous systèmes confondus, la répartition du préjudice pour les transactions nationales en 2009 est la suivante : 2,3 % sont supportés par les porteurs, 41,1 % sont supportés par les établissements émetteurs et acquéreurs et 56,5 % sont supportés par les commerçants, principalement en vente à distance. La part supportée par les commerçants, qui était de 53,5 % en 2008, augmente encore du fait de la croissance de la fraude sur les paiements à distance, qui est très majoritairement supportée par ceux-ci (le coût de la fraude n'est pas supporté par les commerçants lorsqu'ils utilisent des systèmes sécurisés tels que « 3D-Secure »).

De plus, sur les 342,4 millions d'euros de fraude enregistrés par les systèmes français en 2009, on peut estimer qu'environ 94,5 millions d'euros (soit 28 %) seraient supportés par les systèmes étrangers. Ceci découle de l'application des règles internationales de partage de responsabilité dans le cadre de la mise en œuvre du standard EMV et du dispositif d'authentification pour les paiements à distance « 3D-Secure ».

2|4 Répartition de la fraude par type de transaction

La typologie de transaction de paiement par carte adoptée par l'Observatoire distingue les paiements de proximité et sur automate (réalisés au point de vente ou sur distributeurs de carburant, de billets de transport...) des paiements à distance (réalisés sur Internet, par courrier, par téléphone / fax, etc.) et des retraits. Pour une meilleure lisibilité, les développements qui suivent distinguent les données nationales des données internationales.

Transactions nationales

Transactions nationales	Taux de fraude (Montant de la fraude en millions d'euros)				
	2005	2006	2007	2008	2009
Paiements	0,033 % (82,8)	0,035 % (92,3)	0,032 % (95,6)	0,036 % (111,7)	0,038 % (123,2)
- dont paiements de proximité et sur automate	0,025 % (59,2)	0,024 % (59,1)	0,017 % (45,4)	0,015 % (44,5)	0,014 % (41,0)
- dont paiements à distance	0,196 % (23,6)	0,199 % (33,2)	0,236 % (50,1)	0,252 % (67,2)	0,263 % (82,2)
- dont par courrier / téléphone	nd	0,194 % (19,8)	0,201 % (23,8)	0,280 % (28,5)	0,263 % (30,3)
- dont sur Internet	nd	0,208 % (13,4)	0,281 % (26,4)	0,235 % (38,8)	0,263 % (51,9)
Retraits	0,017 % (15,0)	0,019 % (17,4)	0,020 % (19,0)	0,018 % (19,1)	0,019 % (20,8)
Total	0,029 % (97,8)	0,031 % (109,6)	0,029 % (114,5)	0,031 % (130,9)	0,033 % (144,0)

Source : Observatoire de la sécurité des cartes de paiement

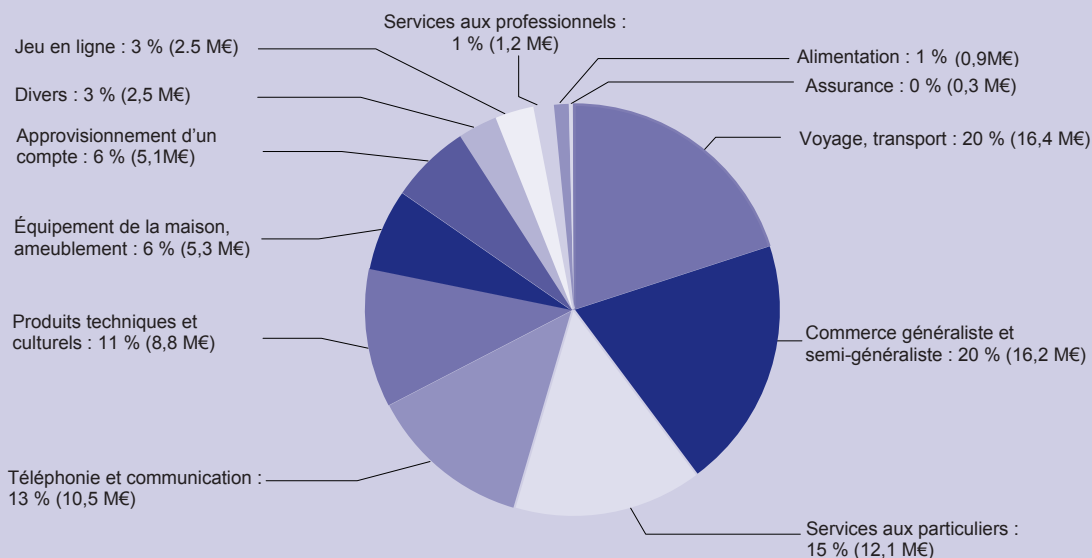
▲ Tableau 5 – Répartition de la fraude nationale par type de transaction

En ce qui concerne les transactions nationales, on observe que :

- le taux de fraude sur les paiements de proximité et sur automate continue de diminuer et s'établit à 0,014 %, pour un montant de fraude de 41,0 millions d'euros (contre 0,015 % et 44,5 millions d'euros en 2008). Les paiements de proximité et sur automate comptent pour 67 % du montant des transactions nationales, et pour seulement 28 % du montant de la fraude ;
- le taux de fraude sur les paiements à distance est de nouveau en hausse en 2009 et s'établit à 0,263 % pour un montant de fraude de 82,2 millions d'euros (contre 0,252 % en 2008, pour un montant de fraude de 67,2 millions d'euros). Les paiements à distance, qui représentent 7 % de la valeur des transactions nationales, comptent ainsi désormais pour 57 % du montant de la fraude. Si cette hausse de la fraude est à relativiser compte tenu de la croissance soutenue du volume et de la valeur des paiements à distance (+ 17,1 % entre 2008 et 2009 en valeur, avec notamment 19,7 % de croissance pour les paiements sur Internet), le niveau très élevé de la fraude sur ce canal de paiement conduit l'Observatoire à encourager la mise en œuvre de mesures permettant de lutter contre cette tendance. Le précédent rapport de l'Observatoire avait souligné l'importance de généraliser progressivement l'authentification du porteur pour tout acte de paiement et de renforcer les méthodes d'authentification utilisées. A ce propos, l'Observatoire rend compte dans le présent rapport (cf. chapitre 4) des résultats d'une étude qualitative sur la perception de la sécurité des transactions en ligne par les porteurs et de l'accueil réservé à différents dispositifs d'authentification non rejouable ;
- le taux de fraude sur les retraits est stable à seulement 0,019 %, pour un montant de fraude de 20,8 millions d'euros (contre 0,018 % en 2008, pour un montant de fraude de 19,1 millions d'euros). Les retraits représentent 25 % du montant des transactions nationales et comptent pour 14 % du montant de la fraude.

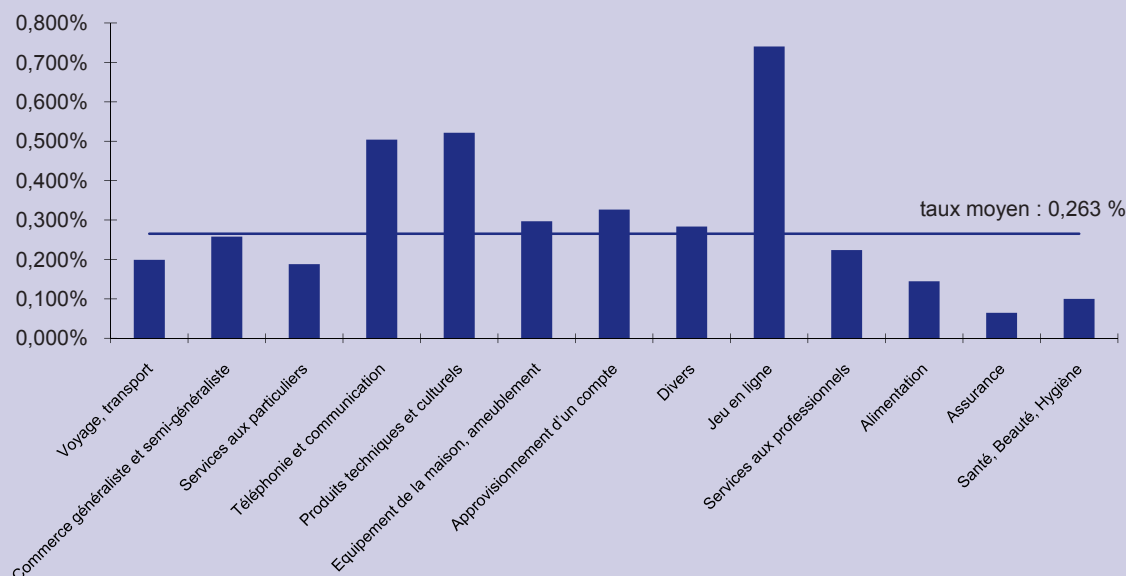
Encadré 5 – Fraude nationale en vente à distance selon le secteur d'activité

L'Observatoire a collecté des données permettant de fournir des indications sur la segmentation de la fraude par secteur d'activité pour les paiements à distance. Ces chiffres ne portent que sur les transactions nationales.



Ventilation de la fraude sur les paiements à distance par secteur d'activité pour les transactions nationales (montant de la fraude en millions d'euros)

Les secteurs Voyage/transport, Commerce généraliste et semi-généraliste et Services aux particuliers représentent 55 % de la fraude, apparaissant ainsi comme les plus exposés. La comparaison des taux moyens de chacun des secteurs d'activité complète cette information et permet de constater que certains secteurs, qui comptent pour une faible part du total de la fraude, subissent toutefois une exposition élevée (Produits techniques et culturels, Jeu en ligne) (cf. histogramme ci-après). Néanmoins, l'Observatoire remarque qu'au sein d'un même secteur, le taux de fraude varie sensiblement d'un commerçant à l'autre selon les mesures de sécurité déployées.



Taux de fraude sur les paiements à distance par secteur d'activité pour les transactions nationales

Source : Observatoire de la sécurité des cartes de paiement

Transactions internationales

		Taux de fraude (Montant de la fraude en millions d'euros)			
Émetteur français – Acquéreur étranger	2006	2007	2008	2009	
Paiements	0,421 % (54,0)	0,483 % (65,2)	0,655 % (99,3)	0,679 % (105,2)	
- dont paiements de proximité et sur automate	0,288 % (28,1)	0,299 % (30,0)	0,286 % (32,0)	0,406 % (44,7)	
- dont paiements à distance	0,840 % (26,0)	1,024 % (35,1)	1,698 % (67,2)	1,350 % (60,5)	
- dont par courrier / téléphone	0,684 % (5,7)	0,790 % (7,6)	1,284 % (11,2)	1,016 % (9,7)	
- dont sur Internet	0,898 % (20,3)	1,117 % (27,4)	1,815 % (56,0)	1,440 % (50,8)	
Retraits	0,555 % (22,4)	0,455 % (20,0)	0,399 % (19,1)	0,331 % (16,5)	
Total	0,453 % (76,4)	0,476 % (85,3)	0,594 % (118,3)	0,594 % (121,6)	
Émetteur étranger – Acquéreur français	2006	2007	2008	2009	
Paiements	0,344 % (61,5)	0,334 % (62,8)	0,339 % (65,4)	0,397 % (74,1)	
Retraits	0,107 % (5,0)	0,117 % (5,9)	0,110 % (5,6)	0,055 % (2,8)	
Total	0,295 % (66,5)	0,288 % (68,7)	0,291 % (71,0)	0,324 % (76,8)	

Source : Observatoire de la sécurité des cartes de paiement

▲ Tableau 6 – Répartition de la fraude internationale par type de transaction

En ce qui concerne les transactions internationales, l'Observatoire ne dispose d'une décomposition fine de la fraude par type de transaction que pour les seules transactions réalisées par des cartes françaises à l'étranger. On remarque que la fraude a augmenté sur les paiements de proximité et sur automate (44,7 millions d'euros en 2009 contre 32,0 millions d'euros en 2008) alors qu'elle a légèrement diminué sur les paiements à distance (60,5 millions d'euros en 2009 contre 67,2 millions d'euros en 2008). Néanmoins, on constate toujours un taux de fraude sur les paiements à distance particulièrement élevé (1,350 %) et beaucoup plus important que celui sur les paiements de proximité et sur automate (0,406 %). Le déploiement de dispositifs d'authentification renforcée devrait permettre de limiter la fraude sur les paiements à distance qui, sur cette zone géographique, représentent 22 % des transactions mais 50 % de la fraude.

Enfin, on remarque une diminution de la fraude sur les retraits, tant en montant qu'en taux, qu'il s'agisse de transactions réalisées par des cartes françaises à l'étranger ou par des cartes étrangères en France.

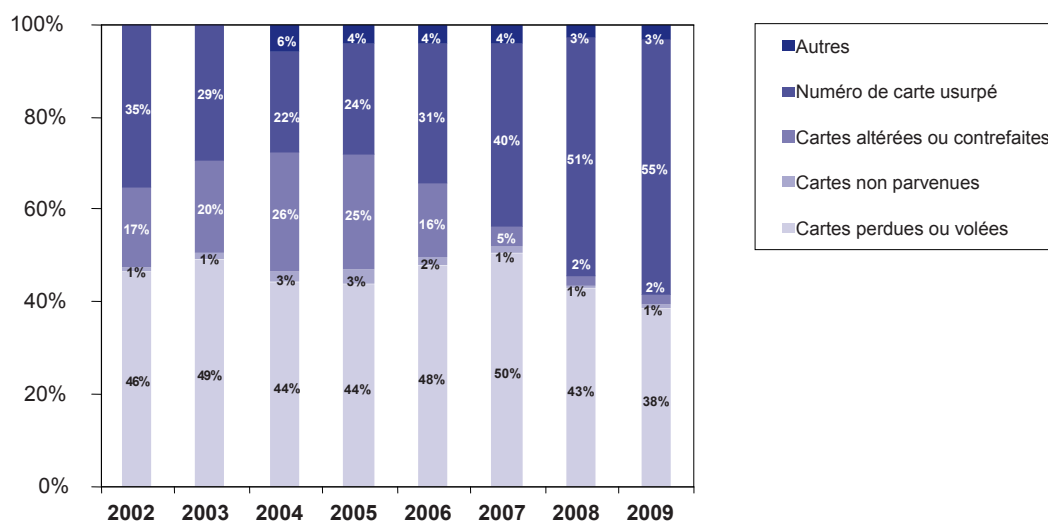
2 | 5 Répartition de la fraude selon son origine

La typologie définie par l'Observatoire distingue les origines de fraude suivantes :

- carte perdue ou volée : le fraudeur utilise une carte de paiement obtenue à l'insu de son titulaire légitime, suite à une perte ou un vol ;
- carte non parvenue : la carte a été interceptée lors de son envoi par l'émetteur à son titulaire légitime ;

- carte falsifiée ou contrefaite : une carte de paiement authentique est falsifiée par modification des données magnétiques, d'embossage ou de programmation ; une carte entièrement fautive est réalisée à partir de données recueillies par le fraudeur ;
- numéro de carte usurpé : le numéro de carte d'un porteur est relevé à son insu ou créé par « moulinage » (à l'aide de générateurs aléatoires de numéros de carte) et utilisé ensuite en vente à distance ;
- une catégorie « autres », qui regroupe, en particulier pour les cartes de type « privatif », la fraude liée à l'ouverture frauduleuse de compte par usurpation d'identité.

L'histogramme suivant indique les évolutions constatées dans ce domaine au niveau national pour l'ensemble des cartes de paiement (la répartition porte uniquement sur les paiements).



Source : Observatoire de la sécurité des cartes de paiement

▲ Tableau 7 – Répartition de la fraude selon son origine (transactions nationales, en valeur)

En augmentation depuis 2005, l'origine de fraude la plus importante (55,1 %, contre 51,3 % en 2008) est celle liée aux numéros de cartes usurpés, utilisés pour les paiements frauduleux à distance. La fraude liée aux pertes et vols de cartes représente encore 38,2 % des paiements nationaux frauduleux. La contrefaçon de cartes n'est plus à l'origine que de 2,2 % des paiements nationaux frauduleux. Enfin, on observe une stabilité de la rubrique « autres », qui est généralement utilisée par les systèmes de carte de type « privatif » pour indiquer les fraudes par ouverture frauduleuse d'un compte ou d'un dossier de crédit (fausse identité) et qui est très significative pour ce type de carte (près de 50 %).

2009	Tous types de cartes		Cartes de type « interbancaire »		Cartes de type « privé »	
	Montant (millions d'euros)	Part	Montant (millions d'euros)	Part	Montant (millions d'euros)	Part
Carte perdue ou volée	55,0	38,2 %	52,6	39,2 %	2,4	25,1 %
Carte non parvenue	1,7	1,2 %	0,8	0,6 %	0,9	9,9 %
Carte altérée ou contrefaite	3,2	2,2 %	2,2	1,7 %	1,0	10,4 %
Numéro usurpé	79,4	55,1 %	78,8	58,6 %	0,6	6,2 %
Autres	4,6	3,2 %	-	-	4,6	48,4 %
Total	144,0	100 %	134,4	100 %	9,6	100 %

Source : Observatoire de la sécurité des cartes de paiement

▲ **Tableau 8 – Répartition de la fraude nationale selon son origine et par type de carte**

Encadré 6 – Indicateurs des services de police et de gendarmerie

Pour l'année 2009, les services de police et de gendarmerie enregistrent une hausse des interpellations pour les fraudes à la carte bancaire, faisant état de 200 personnes interpellées contre 154 en 2008.

Les attaques de distributeurs automatiques de billets (DAB) diminuent avec 411 piratages de DAB en 2009 (contre 427 en 2008, 391 en 2007, 515 en 2006, 200 en 2005 et 80 en 2004). A celles-ci s'ajoutent 1 attaque sur un distributeur automatique de carburant (DAC) (contre 3 en 2008) et 18 attaques de terminaux de paiement (contre 17 en 2008).

Face à de tels agissements, de nombreuses enquêtes ont été diligentées sur l'ensemble du territoire national. On peut distinguer parmi celles-ci :

- l'interpellation d'une équipe de treize personnes spécialisée dans la captation de données de carte, la contrefaçon et l'utilisation de cartes dans des commerces complices en France. Le préjudice est estimé à plus de 200 000 euros ;
- l'interpellation d'une équipe de quatre personnes spécialisée dans la captation de données de cartes aux distributeurs automatiques de billets. De nombreuses données de carte ont été compromises sur une dizaine de distributeurs pour un préjudice total dépassant 250 000 euros ;
- le démantèlement d'une équipe franco-roumaine de neuf personnes spécialisée dans l'utilisation de cartes contrefaites. Les perquisitions ont permis de trouver une dizaine de ces cartes, du matériel utilisé pour la fraude ainsi que 15 000 euros en espèces.

3 | VEILLE TECHNOLOGIQUE

3|1 Suivi de la mise en œuvre des solutions de paiement sans contact (par carte et mobile)

L'Observatoire a publié dans son rapport 2007 une étude portant sur *la sécurité des nouveaux mécanismes d'initiation du paiement par carte (paiement par téléphone mobile, carte sans contact)*¹¹ dans la continuité d'une première analyse publiée en 2004.

Même s'ils sont déjà largement déployés dans certains pays, notamment au Japon, les paiements utilisant des technologies sans contact ne faisaient l'objet, en 2007, que de projets pilotes en France. Dans ce contexte, l'Observatoire avait émis des recommandations portant sur la sécurité des paiements sans contact par carte, d'une part, et par téléphone mobile, d'autre part.

La situation ayant évolué depuis –les cartes sans contact sont désormais en circulation et les paiements par téléphone mobile font l'objet de pilotes à grande échelle– l'Observatoire a souhaité analyser la situation présente, vérifier que les recommandations qu'il avait émises en 2007 ont bien été suivies par les émetteurs et accepteurs¹² et analyser l'adéquation de ces recommandations au contexte actuel.

Caractéristiques et enjeux de sécurité des modes de paiement sans contact

Les modes de paiement sans contact reposent sur l'utilisation d'une carte ou d'un téléphone mobile. Dans les deux cas, ces éléments communiquent avec les terminaux de paiement à l'aide d'une antenne permettant d'émettre des communications selon le protocole « NFC » (Near Field Communication), lequel est prévu pour fonctionner à très faible distance, de l'ordre de quelques centimètres. Chaque dispositif a ensuite des caractéristiques qui lui sont propres.

Cartes sans contact

Dans le cas des cartes sans contact, l'application de paiement de la banque émettrice se trouve sur la puce et cohabite avec une application de paiement classique fonctionnant en mode contact. Afin d'accélérer le processus de paiement, la saisie d'un code PIN n'est pas demandée pour un paiement sans contact dans les cas suivants :

- pour les transactions dont le montant unitaire est inférieur à un seuil actuellement de l'ordre de 20 à 30 euros ;
- en-dessous d'un certain montant cumulé ;
- en-dessous d'un certain nombre de transactions prédéfini en mode sans contact.

Dans tous les autres cas, la carte est présentée en mode contact avec contrôle du code PIN.

¹¹ Cf. Rapport annuel 2007, pp.36 à 43. Le champ de ces études couvre les paiements par carte sans contact et par téléphone mobile sans contact.

¹² Comme dans les rapports 2004 et 2007, les cartes prépayées, examinées dans le cadre des travaux de suivi des politiques de sécurité des émetteurs et des accepteurs, ne sont pas couvertes par cette étude.

Ces trois types de données (montant unitaire, montant cumulé, nombre de transactions) sont suivis à l'aide de compteurs, gérés par l'application de paiement et dont la réinitialisation s'opère par une demande d'autorisation avec saisie du code PIN lors d'un paiement en mode contact.

Paiement sans contact par téléphone mobile

En l'état actuel des expérimentations, deux modèles émergent quant au stockage de l'application de paiement dans un « secure element »¹³ au sein du téléphone mobile :

- celle-ci peut être logée dans la puce SIM (Subscriber Identity Module) gérée par l'opérateur téléphonique¹⁴. C'est alors l'application de paiement, au sein de ce microprocesseur, qui exécute les opérations permettant d'initier le paiement ;
- une deuxième solution consiste à loger l'application de paiement dans un « secure element » distinct de la SIM, qui initie la transaction de paiement, contrôle les communications NFC et contient des certificats numériques. Cette architecture permet de développer des services indépendamment des infrastructures des opérateurs de télécommunication, c'est-à-dire sans faire intervenir la carte SIM ni les services associés de téléphonie.

Les banques émettrices de l'application de paiement conservent néanmoins dans les deux cas la maîtrise sécuritaire du composant au sein duquel se trouve leur application, notamment en exigeant des évaluations des composants hôtes et des applications de paiement.

Comme pour les cartes, l'application de paiement gère des seuils de transactions dont l'atteinte impose la saisie d'un « code personnel » sur le clavier du téléphone, indépendant du code PIN d'activation de la carte SIM ou de tout autre « secure element ». L'utilisateur peut choisir de rendre la saisie de ce code systématique, quel que soit le montant de l'achat. Par ailleurs, la remise à zéro des compteurs peut s'effectuer à distance lorsqu'un des seuils est atteint. Ce processus comporte une demande d'autorisation émise par le téléphone et qui nécessite l'accord explicite du client. Celui-ci se matérialise par la saisie de son code personnel lors de cette même demande ou à la première transaction suivante.

* * * *

L'étude de l'Observatoire de 2007 avait identifié quatre types de menaces¹⁵ associées aux modes de paiement sans contact. Les évolutions actuelles liées au déploiement progressif des modes de paiement sans contact renforcent le besoin de prendre en compte ces menaces, dont certaines peuvent par ailleurs être combinées.

Écoute des informations échangées

La communication entre le terminal de paiement et la carte ou le téléphone mobile se faisant par ondes radio, il existe un risque de capture des informations échangées lors du paiement et de leur réutilisation à des fins frauduleuses. Ces informations concernent le numéro de la carte

¹³ Le terme « secure element » couvre ici la SIM ou tout autre composant électronique sécurisé (carte SD, etc.) pouvant héberger une application de paiement.

¹⁴ Le standard « Global Platform » utilisé pour l'architecture des puces SIM prévoit que celles-ci comportent différentes unités isolées, les « Security Domains », permettant d'y inscrire des applications logicielles distinctes.

¹⁵ Écoute des informations échangées, activation de l'application de paiement à l'insu du porteur, vol du support sans contact, attaques contre l'application de paiement.

(le PAN)¹⁶, le montant de la transaction et les données d'authentification de la carte ou du « secure element ».

Deux dispositifs permettent cependant de limiter la réutilisation de données capturées. D'une part, l'authentification dynamique, à chaque transaction, de l'application de paiement contenue sur la carte ou dans le téléphone mobile permet de sécuriser la connexion entre le support sans contact et le terminal. D'autre part, l'utilisation d'un PAN dédié au mode sans contact (distinct du PAN de la carte de paiement lorsque celle-ci est utilisée en mode contact ou en vente à distance) pourrait garantir que cet identifiant ne puisse pas être réutilisé par d'autres modes d'acceptation s'il venait à être intercepté.

Par ailleurs, concernant la communication entre les terminaux de paiement et les serveurs d'acquisition et d'autorisation, la réutilisation des infrastructures pour les cartes de paiement à contact permet de bénéficier des protections déjà existantes.

Activation de l'application de paiement à l'insu du porteur

L'utilisation d'une interface sans contact rend possible l'établissement d'un dialogue avec la carte ou le téléphone mobile du porteur sans son consentement. Ceci peut conduire à différents types d'actions dommageables pour chacun des supports utilisés.

Cartes sans contact

Le mode sans contact permet d'envisager la réalisation de transactions à l'insu du porteur, notamment pour des transactions inférieures à un seuil actuellement autour de 20-30 euros où le code PIN n'est pas saisi (« télé-pickpocketing »). La limitation de la distance entre le support sans contact et le terminal réduit toutefois la possibilité d'activer un support sans contact avec un terminal frauduleux. L'Observatoire recommandait néanmoins dès 2007 la mise en œuvre de processus d'activation et désactivation du mode sans contact afin de s'assurer du consentement du porteur lors de chaque transaction. L'utilisation d'étuis protecteurs visant à bloquer les ondes radio et à interdire tout accès à l'application de paiement en dehors des courts intervalles de paiement durant lesquels le payeur retirerait sa carte de l'étui entre notamment dans ce cadre.

Paiement sans contact par téléphone mobile

Seule une fonction d'activation et de désactivation de l'application de paiement utilisant le clavier intégré du téléphone assurerait un niveau de sécurité équivalent à celui décrit précédemment pour les cartes sans contact.

Concernant la sécurisation de la remise à zéro des compteurs de transaction, le fait de saisir le code personnel pour réinitialiser ces compteurs permet de s'assurer de l'authentification du porteur. La remise à zéro des compteurs à distance par sa banque nécessite quant à elle de prévoir un canal sécurisé entre le téléphone mobile et la banque (notamment si l'envoi d'information se fait par SMS via l'opérateur téléphonique) et des contrôles de flux stricts au niveau de la banque (contrôle de la légitimité des réinitialisations de compteurs, limitation en nombre sur une période donnée pour un téléphone donné...).

¹⁶ « Primary Account Number » : données qui identifient l'émetteur de la carte et le numéro de la carte.

Vol du support sans contact

La carte et le mobile sans contact sont sensibles au vol dans la mesure où, en l'absence de saisie du code PIN (respectivement du code personnel) et de vérification en ligne de la validité de la carte (respectivement de l'application de paiement du mobile), il est possible d'utiliser un support volé pour des achats de petit montant.

Toutefois, l'existence de seuils de montants maximaux pouvant être payés sans contact permet de limiter le préjudice financier en cas de fraude. L'installation de compteurs dans l'application de paiement permet de calculer le montant cumulé des opérations de petite valeur et d'imposer au porteur de saisir son code PIN ou son code personnel avec son téléphone mobile pour les remettre à zéro.

En outre, en cas de vol, la mise en opposition de la carte sans contact ou de l'application de paiement du mobile doit permettre de faire cesser toute utilisation frauduleuse. Pour les téléphones mobiles, le blocage de l'application peut se faire grâce à la technologie OTA¹⁷, qui permet la mise à jour à distance de l'application.

Attaques contre l'application de paiement

D'éventuelles attaques peuvent être menées contre l'application de paiement, que celle-ci soit inscrite sur la puce d'une carte ou contenue dans le « secure element » d'un téléphone mobile. Si les cartes font aujourd'hui l'objet d'une certification sécuritaire, la possibilité d'attaques contre la puce contenant l'application de paiement dans les téléphones mobiles souligne la nécessité d'établir un processus similaire pour les composants de cette puce, mené par un tiers indépendant comme l'avait recommandé l'Observatoire en 2007.

Le niveau de sécurité induit devrait permettre de s'assurer que l'application de paiement ainsi que les données qu'elle contient sont protégées de façon adéquate, et bénéficient à ce titre d'un cloisonnement par rapport aux autres applications et d'un accès restreint au cadre des transactions autorisées. A cet égard, les standards de sécurité établis par exemple par le consortium « GlobalPlatform » pour les puces SIM permettent de s'assurer de ce cloisonnement entre applications. De plus, les évaluations sécuritaires effectuées dans le cadre du schéma de certification national¹⁸ garantissent un haut niveau de sécurité de ces applications ainsi que des composants utilisés.

Le téléphone mobile peut en outre lui-même être exposé à des risques de transmission de logiciels malveillants (capture de données, simulation d'application de paiement à des fins de « phishing », etc.) par des canaux de communication variés (Bluetooth, Wifi, GSM par exemple). On notera toutefois que les démarches relatives à la sécurisation du paiement par mobile considèrent ce dernier comme « transparent » en termes de sécurité et visent à protéger les applications de paiement ainsi que leur seul support, sans reposer sur la sécurité de l'appareil en lui-même.

Enfin, les applications de paiement sans contact utilisant des secrets pouvant être compromis dans les chaînes de fabrication ou de personnalisation des composants, il apparaît nécessaire que les différents acteurs de la monétique appliquent au paiement sans contact les mêmes règles de gestion des secrets que pour les cartes de paiement fonctionnant en mode contact.

¹⁷ La technologie OTA (« Over The Air ») permet d'accéder aux données figurant sur la carte SIM à distance et de mettre à jour ces données de façon sécurisée.

¹⁸ ANSSI

État des lieux du paiement sans contact

Les initiatives en cours

Le paiement sans contact s'est développé en France depuis 2007, passant de prototypes au lancement de projets pilotes voire à la commercialisation de produits.

Cartes sans contact

L'essentiel de la commercialisation des cartes sans contact est le fait de la Société des Paiements Pass (S2P). Celle-ci a déployé 2,5 millions de cartes Pass sans contact en 2009, acceptées dans les magasins Carrefour. Moneo, à travers la société BMS (Billettique Monétique Services) a également développé des porte-monnaie électroniques sous forme de cartes sans contact depuis 2006. 500 000 cartes sont déjà en circulation, acceptées notamment dans les CROUS.

Moneo a, en outre, développé un nouveau mode de paiement sans contact, sous forme de clé USB sans contact (Smart Object Weneo/Moneo). Ce mode de paiement sans contact est déjà expérimenté à Bordeaux depuis 2009 et à Toulon depuis février 2010.

Enfin, les cartes de paiement sans contact Visa « Pay Wave » et MasterCard « PayPass » ont également été lancées en test dans les villes de Caen et Strasbourg depuis septembre 2009. Ces cartes ne connaissent toutefois pour l'instant qu'un déploiement limité (1 000 cartes émises).

Paiement sans contact par téléphone mobile

Le paiement sans contact par téléphone mobile est encore davantage, en 2010, au stade de l'expérimentation que de la commercialisation.

Moneo teste des solutions de paiement par porte-monnaie électronique sur téléphone mobile. Le projet *Nice Futur Campus* prévoit ainsi le déploiement de 300 mobiles équipés de la technologie NFC en 2010 qui feront office de carte étudiante virtuelle multiservices et qui permettront, notamment, de payer de petits montants.

Le projet Pegasus, lancé en 2007 a quant à lui permis de définir des spécifications permettant le fonctionnement d'une application de paiement sur la carte SIM d'un téléphone mobile. Ce projet associait banques, opérateurs de téléphonie mobile, constructeurs de terminaux et systèmes de cartes internationaux. Des tests ont été menés dans ce cadre à Caen et Strasbourg en 2007 et 2008. La continuité de ce projet, à une plus grande échelle, est désormais assurée par l'initiative « Nice, Territoire d'Innovation » (cf. infra).

L'initiative « Nice, Territoire d'Innovation »

Cette initiative est conçue comme un test grandeur nature pour le développement futur de la technologie sans contact sur carte et téléphone mobile. Elle regroupe les principaux opérateurs de téléphonie mobile, les banques, des prestataires techniques, ainsi que des collectivités locales et des entreprises. Les quelques trois mille téléphones équipés de la technologie NFC¹⁹ et déployés au deuxième trimestre 2010 sur le territoire de Nice Côte d'Azur permettront à la

¹⁹ Technologie de communication par ondes radio sur très courtes distances (quelques cms).

fois de réaliser des paiements de proximité et d'accéder à d'autres services (transport, billetterie, carte de fidélité, contrôle d'accès, information). Ce projet vise également à servir de tremplin au mode de paiement sans contact par carte et à déployer un réseau d'acceptation de terminaux de paiement sans contact auprès des commerçants.

L'impact des évolutions technologiques récentes

Cartes sans contact

La majorité des cartes déployées aujourd'hui a fait l'objet de spécifications techniques qui n'ont que peu évolué depuis les dernières recommandations de l'Observatoire. On notera cependant quelques initiatives visant à introduire un clavier sur les cartes elles-mêmes ou à signaler au porteur l'activation ou non de sa carte. Ces projets permettraient aux cartes de bénéficier de fonctionnalités réservées jusqu'à présent aux téléphones mobiles, mais se heurtent encore à des obstacles techniques, principalement liés à l'alimentation et à l'autonomie des cartes.

Paiement sans contact par téléphone mobile

L'utilisation accrue des téléphones mobiles ainsi que le développement des fonctionnalités des « smartphones » accroissent les risques d'attaques sur ce segment. Différentes mesures peuvent toutefois limiter leur impact :

- la mise en place de signatures des logiciels mobiles²⁰ permet de différencier strictement l'application de paiement des autres applications sur le mobile ;
- le filtrage des communications peut être effectué, afin d'isoler celles destinées à l'application de paiement ;
- des études sont également en cours sur la mise en œuvre de modes sécurisés qui seraient déclenchés lors d'un paiement sur mobile. Ces modes permettraient de protéger l'interaction du porteur avec l'application de paiement, en s'assurant notamment de l'intégrité des données entrées sur le clavier et affichées sur l'écran du téléphone.

Par ailleurs, ce mode de paiement introduit de nouveaux acteurs, les « Trusted Service Managers » (TSM), ce qui accroît d'autant les flux d'informations et la nécessité de mettre en place des mesures de sécurité propres à assurer l'intégrité et la confidentialité des données échangées. Les TSM assurent en effet le lien entre les émetteurs et les téléphones mobiles lors des opérations de personnalisation de l'application de paiement (cycle de vie) ou de réinitialisation des compteurs. Ils se placent en tiers de confiance et se doivent donc de garantir le maintien d'un haut niveau de sécurité tout au long de ces opérations.

Plus généralement, les projets ou expérimentations en cours visent, avant tout déploiement de masse sur le territoire français, à affiner les spécifications techniques propres au paiement par téléphone mobile sans contact, notamment concernant la partie sécuritaire. Dans cette optique, une convergence des travaux menés d'une part par l'AEPM²¹, d'autre part par les réseaux internationaux (Visa, Mastercard) est actuellement en cours.

²⁰ Il s'agit des « Cardlets » pour les applications de paiement et des « Midlets » pour les interfaces entre le téléphone et l'utilisateur. Les premières sont stockées dans le « secure element », les secondes dans le téléphone mobile.

²¹ Association Européenne Payez Mobile, créée en octobre 2008 et regroupant des banques et opérateurs de télécommunications à l'origine du paiement sans contact sur mobile en France. L'AEPM assure la continuité du projet Pegasus.

Recommandations additionnelles formulées par l'Observatoire

En 2007, l'Observatoire avait conclu que les risques spécifiques au paiement sans contact étaient liés d'une part à l'échange des données de la transaction par ondes radio, et d'autre part, à l'absence de validation de la transaction en dessous de certains montants qui ne permet pas d'authentifier le porteur.

Par conséquent, l'Observatoire avait émis deux axes de recommandations à propos du paiement sans contact, à savoir la possibilité d'une part de mettre en place des mesures permettant de s'assurer du consentement du porteur, et d'autre part de garantir un niveau de sécurité élevé des composants et applications utilisés.

En ce qui concerne les cartes sans contact, les recommandations de 2007 de l'Observatoire ont été suivies par les émetteurs.

Pour les paiements sans contact par téléphone mobile, les projets et pilotes actuels prévoient d'affiner les mécanismes sécuritaires nécessaires au déploiement en masse. Il conviendra de s'assurer que l'ensemble de ces mesures est également mis en œuvre lors de la commercialisation à grande échelle de modes de paiement innovants sans contact.

L'Observatoire recommande en outre de poursuivre les études et la mise en œuvre de pratiques sécuritaires sur les cartes et les téléphones mobiles sans contact propres à garantir un niveau de confiance élevé dans ces instruments de paiement.

L'utilisation d'un PAN dédié au mode sans contact (distinct du PAN de la carte de paiement lorsque celle-ci est utilisée en mode contact ou en vente à distance) entre notamment dans ce cadre. Elle permettrait en effet de limiter les impacts potentiels d'une réutilisation de cet identifiant sur d'autres environnements en cas de compromission.

Dans le cas des téléphones mobiles, l'Observatoire préconise :

- la fourniture d'un code personnel de paiement différent du code PIN d'activation de la carte SIM, ainsi que du code confidentiel des cartes de paiement de l'utilisateur. Lorsque ce code personnel est modifiable par l'utilisateur, l'émetteur bancaire doit lui recommander d'en utiliser un différent des autres codes en sa possession ;
- l'utilisation de composants dont le niveau de sécurité est au moins égal à celui des puces utilisées dans les cartes en mode contact ;
- que les acteurs concernés étudient la possibilité de renforcer la protection de l'interaction du porteur avec l'application de paiement sur le téléphone mobile ;
- que les acteurs impliqués dans l'ensemble des opérations liées au paiement sans contact par téléphone mobile (paiement lui-même, mais également personnalisation/mise à jour des applications et remise à zéro des compteurs de transactions à distance) mettent en œuvre des mesures de protection cryptographiques garantissant l'intégrité et la confidentialité des données échangées entre les systèmes.

Concernant les cartes sans contact, il conviendra pour les émetteurs de poursuivre l'étude de solutions simples permettant d'activer et désactiver le mode de paiement sans contact, à l'image des étuis protecteurs existants.

L'Observatoire continuera à exercer une veille technologique sur ces solutions de paiement innovantes afin de tenir compte de la finalisation de leurs spécifications et de leurs développements par les professionnels.

3|2 Sécurité du paiement à distance par courrier et téléphone

La forte croissance de la vente à distance ces dernières années s'accompagne d'un net accroissement des paiements par carte à distance. Toutefois, l'observation des flux tant du commerce électronique sur Internet, que de la vente par correspondance ou par téléphone²² montre des évolutions contrastées. En 2008, la croissance des paiements par carte sur Internet se poursuivait tandis que les paiements par carte par courrier ou téléphone (« Mail order/Telephone order » - MO/TO) étaient en diminution sensible, sans doute en raison de l'usage croissant d'Internet pour la vente par correspondance. Ainsi, 109 millions de paiements par carte reçus par courrier ou par téléphone ont été enregistrés en 2008, représentant près de 10 milliards d'euros (environ 2 % de la valeur des transactions nationales). Le paiement à distance par courrier et téléphone répond à certains besoins précis des consommateurs et des commerçants. Les coupons de vente à distance par courrier sont en particulier utilisés pour des abonnements à des journaux et pour la vente par correspondance, notamment par des porteurs ne disposant pas d'un accès à Internet. Le paiement à distance par téléphone correspond souvent à des transactions urgentes, comme la réservation de chambres d'hôtel, de spectacles ou de taxis.

L'Observatoire a constaté ces dernières années un taux de fraude bien plus élevé sur les paiements à distance que sur les paiements de proximité et sur automate. Le rapport de 2008 a permis de faire le point des mesures de sécurité mises en œuvre pour les paiements par carte réalisés par Internet. L'objet de la présente fiche est d'analyser les questions de sécurité des paiements à distance par courrier et téléphone.

Les mesures de sécurité appliquées au paiement à distance par courrier et téléphone

Dans l'analyse des questions de sécurité du paiement à distance, il convient de distinguer :

- d'une part, la protection des données de carte (numéro, date d'expiration, cryptogramme visuel) reçues au travers du canal de communication et qui sont ensuite utilisées dans l'environnement du commerçant, puis de sa banque, voire dans celui de tout prestataire technique auquel l'un ou l'autre pourrait avoir recours. Ces données, si elles venaient à être récupérées par un fraudeur²³, pourraient être réutilisées en vue de réaliser un paiement frauduleux. C'est la raison pour laquelle la protection de ces données, tant lors de leur transmission sur les canaux servant à leur échange (informatique, courrier, Internet), que lors de leur utilisation et de leur éventuelle conservation, est cruciale. Il existe un certain nombre de préconisations réglementaires, posées par la CNIL en France, ou professionnelles –notamment les standards PCI DSS des réseaux de carte internationaux Visa et MasterCard. Cette question fait l'objet dans le présent rapport d'une étude particulière au titre du suivi des politiques de sécurité des émetteurs et des accepteurs. En conséquence, la présente fiche ne traite pas de ce sujet ;
- d'autre part, la lutte contre la réalisation de paiements frauduleux à distance avec des données de carte usurpées, quel que soit le moyen ayant permis cette usurpation (vol de la



²² Le paiement par téléphone qui est visé ici s'entend comme celui qui est effectué par simple appel téléphonique et non par échange de données comme cela commence à apparaître avec des solutions innovantes (paiement mobile).

²³ On parle dans ce cas de « compromission » des données.

carte, copie des données, moulinage, etc.). C'est ce phénomène qu'illustrent les chiffres de fraude calculés par l'Observatoire. Pour 2008, il a été relevé un accroissement du taux de fraude pour les paiements par carte par courrier et téléphone : celui-ci était en effet de 0,280 % contre 0,201 % l'année précédente. Pour la première fois en 2008, le taux de fraude national pour le canal MO/TO dépassait le taux de fraude sur Internet. La réalisation de la fraude en paiement par courrier et par téléphone pose la question de la détection des transactions suspectes et de la vérification que l'acheteur est bien le porteur légitime de la carte. La présente fiche vise à décrire l'ensemble des mesures mises en œuvre en la matière.

Les différentes étapes du paiement à distance par courrier et téléphone sont présentées dans l'encadré ci-dessous :

Encadré 7 – Principes du paiement à distance par courrier et téléphone

Canal		
Porteur	Le porteur remplit et poste un coupon d'achat. Celui-ci inclut notamment le nom du porteur, le numéro de la carte, sa date d'expiration et le code CVx2.	Le porteur appelle le numéro fourni par le commerçant, et paye en indiquant à un opérateur ou à un serveur vocal les mêmes informations.
Commerçant (ou prestataire)	La Poste transmet le courrier, généralement à un prestataire, qui assure la saisie de la commande et des données du paiement et transmet ces dernières à l'acquéreur. Certaines de ces données sont également conservées.	Un opérateur ou un serveur vocal, généralement fourni par un prestataire du commerçant, reçoit les données du paiement et les transmet à l'acquéreur. Certaines de ces données sont également conservées.
Acquéreur	L'acquéreur reçoit l'ordre électronique de paiement et le transmet à la banque émettrice.	
Banque émettrice	La banque émettrice reçoit l'ordre de paiement, fait les vérifications nécessaires puis autorise la transaction.	
La protection des données de paiement par le commerçant fait l'objet de prescriptions des standards PCI DSS ²⁴ et est hors du champ de cette étude.		

²⁴ Ces standards sont établis par conjointement par American Express, Discover Financial Services, JCB International, MasterCard Worldwide, et Visa, Inc.

Les solutions de sécurité

Le groupe « Veille technologique » a examiné les différentes solutions qui permettent de s'assurer de l'authenticité du paiement à distance par courrier et téléphone.

Les procédures de détection de transactions suspectes mises en œuvre par les commerçants consistent à croiser un certain nombre d'indications et de paramètres relatifs au bien ou au service acheté, à l'acheteur, à ses données de paiement ou encore à l'adresse de livraison. Elles permettent par la technique du faisceau d'indices, de donner au commerçant une assurance plus ou moins grande que la transaction ne présente pas le risque d'être payée de façon frauduleuse. De telles procédures existent pour les paiements par Internet ; elles sont adaptées au canal de communication utilisé dans le cas des paiements par carte effectués par courrier ou par téléphone. Certains acteurs traditionnels de la vente par correspondance disposent d'une expertise reconnue dans la mise en œuvre de ce type de procédure et peuvent ainsi réussir à faire échec à des tentatives de fraude. Toutefois, tous les commerçants ne disposent pas de telles procédures, notamment parce que celles-ci supposent généralement des moyens humains ou techniques relativement coûteux. Les commerçants peuvent recourir à des services d'assurance pour se protéger de la fraude. Sauf à s'appuyer sur des procédures de détection de transactions suspectes, de tels services ne sont pas couverts ici.

La vérification du cryptogramme visuel, qui a été introduit pour les cartes de type interbancaire il y a plusieurs années²⁵, permet de donner une meilleure assurance que l'acheteur était normalement en possession de la carte dont le numéro et la date d'expiration sont utilisés pour payer. La vérification de ce cryptogramme est imposée par les systèmes de paiement par carte à l'ensemble des commerçants acceptant en France des paiements à distance. Tout en ayant prouvé son utilité, cette protection n'a pas éliminé tout risque de fraude dans la mesure où certains fraudeurs peuvent avoir détourné cette information en même temps que les autres données de la carte (par exemple lorsque la carte a été perdue ou volée).

La génération aléatoire d'un code à usage unique, comme cela commence à être utilisé pour le paiement par carte sur Internet, a également été examinée par le groupe « Veille technologique ». Le code à usage unique sert au porteur à s'authentifier comme le porteur légitime auprès du commerçant. Contrairement au canal Internet qui permet des vérifications informatiques, il peut être difficile d'utiliser de tels codes pour les canaux MO/TO. Il conviendrait en effet d'empêcher l'utilisation abusive de ce code à usage unique, par exemple par un employé indélicat. A ce stade, il est difficile d'imaginer pouvoir l'employer pour le paiement par carte envoyé par courrier. Les paiements par téléphone sur un serveur vocal, étant exécutés dans un environnement informatisé, pourraient offrir une meilleure garantie de protection. Le groupe « Veille technologique » marque néanmoins ses réserves quant à la possibilité de mettre en place ce type de solution de manière correctement sécurisée.

Le groupe « Veille technologique » note que les solutions en place permettent au commerçant d'éviter un certain nombre de tentatives de fraude, mais qu'elles ne peuvent en tant que telles permettre d'authentifier l'acheteur comme porteur légitime d'une carte. L'exposition à la fraude risque donc de rester élevée et le groupe « Veille technologique » suggère que ce type de paiement soit employé avec précaution. Il propose de formuler un certain nombre de conseils et de bonnes pratiques pour les porteurs et pour les commerçants utilisant ce type de paiement.

²⁵ Voir rapport annuel 2004 de l'Observatoire de la sécurité des cartes de paiement.

Conclusion et propositions de recommandations

Pour la sécurité des paiements par carte, par courrier, ou par téléphone, le groupe « Veille technologique » note l'importance d'un comportement prudent tant de la part des commerçants que de la part des porteurs.

Pour les commerçants, l'Observatoire recommande en particulier les bonnes pratiques suivantes :

- chaque fois que cela est possible pour la vente à distance, le commerçant devrait privilégier la réalisation du paiement au travers d'un canal informatisé comme l'Internet plutôt que par courrier ou par téléphone, afin de mieux pouvoir authentifier le porteur de la carte ;
- le commerçant recueillant des paiements par courrier ou téléphone est appelé à être vigilant quant aux mesures de sécurité qu'il applique, notamment s'il vend des biens ou des services particulièrement prisés par les fraudeurs. Il peut par exemple être attentif à la cohérence des informations fournies par l'acheteur (contrôle de l'adresse de livraison par exemple). Il est invité à se rapprocher de son prestataire de services de paiement et de sa fédération professionnelle pour disposer des conseils les plus à jour ;
- l'attention des commerçants est rappelée sur le caractère obligatoire du recueil et de la vérification du cryptogramme visuel lorsque celui-ci existe et que le système de paiement par carte le requiert ;
- avant de conclure la vente, notamment pour les transactions de montant élevé, il est conseillé au commerçant de procéder auprès du porteur à quelques vérifications destinées à s'assurer qu'il est bien l'initiateur du paiement, par exemple en l'appelant pour confirmation de sa commande. Au moment de la livraison ou du retrait, il peut veiller à ce que la personne qui prend possession du bien ou du service y est bien habilitée ;
- les commerçants sont incités à ne pas conserver de données sensibles dès lors que celles-ci ne leur sont plus utiles.

Pour les porteurs, l'Observatoire recommande en particulier les bonnes pratiques suivantes :

- avant de transmettre leurs données de carte par courrier ou par téléphone, les porteurs de carte doivent s'assurer qu'ils sont en relation avec un commerçant légitime. Il convient en particulier d'être vigilant à l'encontre de tentatives d'escroqueries, menées par des fraudeurs qui tenteraient d'obtenir les données de la carte contre promesse par exemple d'un bien ou d'un service qui ne serait jamais livré ;
- avant de choisir de transmettre leurs données de carte par courrier ou par téléphone, les porteurs de carte doivent s'assurer d'avoir correctement pris connaissance des conditions contractuelles prévues pour le paiement. En particulier, il convient avant d'autoriser le paiement de vérifier si le contrat prévoit que des débits pourront être effectués de façon récurrente par le commerçant ;
- après leur paiement, les porteurs de cartes sont invités à vérifier sur leur relevé de compte que le montant des débits correspond bien aux achats autorisés. Il est rappelé que la loi protège le porteur en cas d'utilisation frauduleuse de sa carte ou des données de celle-ci ;
- les porteurs doivent veiller à ne jamais transmettre leur code confidentiel (PIN) par courrier ou téléphone.

3|3 Sécurité des nouveaux terminaux de paiement « légers »

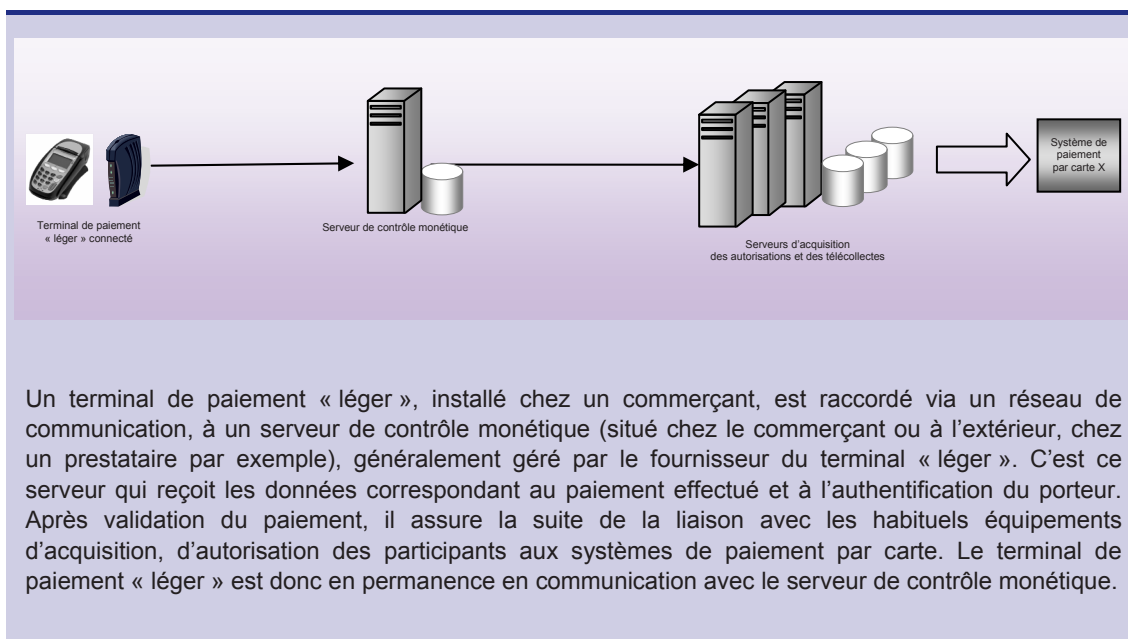
Les terminaux de paiement qui sont aujourd'hui déployés sont des matériels sophistiqués permettant de réaliser de nombreux contrôles monétiques afin de vérifier l'authenticité de la carte et du porteur. Lorsqu'ils interagissent avec la puce d'une carte de paiement, ils mettent en jeu des mécanismes de contrôles cryptographiques complexes, et indiquent si la carte est valide et si le porteur est bien le titulaire de celle-ci. Historiquement, le développement de ces fonctions de contrôle sur les terminaux placés en magasin s'explique par le coût autrefois élevé des communications téléphoniques qu'il aurait fallu réaliser entre le terminal et les sites informatiques des banques. Le développement considérable des réseaux téléphoniques depuis plus de dix ans modifie petit à petit cet équilibre. Le haut débit Internet s'étant généralisé, il devient concevable de ne plus effectuer « en local », c'est-à-dire sur le terminal lui-même, certains des contrôles, mais de réaliser ceux-ci par télécommunication, de manière déportée, sur un serveur distant. Ce concept nouveau vise à simplifier les fonctions de sécurité du terminal, d'où le nom de terminal « léger » qui lui est donné, de manière à en réduire les coûts et contraintes de fabrication puis de déploiement, voire de maintenance. Ce concept récent ne connaît pas encore d'application concrète même s'il fait l'objet de travaux d'étude, voire de premiers pilotes²⁶. Dans le contexte de l'ouverture du marché des services de paiement à de nouveaux opérateurs susceptibles d'offrir des services d'acquisition de transactions de paiement par carte, l'Observatoire a souhaité analyser le fonctionnement d'un terminal « léger », afin de mesurer dans quelles conditions de sécurité celui-ci pourrait être mis en œuvre.

Les caractéristiques sécuritaires des terminaux de paiement « légers »

Le concept de terminal de paiement « léger » consiste à faire exécuter la majeure partie des fonctions de sécurité, non plus sur le terminal lui-même, mais sur un serveur distant auquel il est connecté en permanence. Par rapport au mode de fonctionnement d'un terminal classique, lui aussi connecté pour la collecte, le plus souvent journalière, des transactions acceptées et pour l'envoi des demandes d'autorisation, le changement principal consiste à faire réaliser à distance des contrôles cryptographiques destinés à vérifier l'authenticité de la carte et du porteur. Ceci permet d'alléger certains composants du terminal afin de diminuer les coûts. Cela offre également l'avantage de faciliter la gestion des changements applicatifs qui peuvent être effectués de manière centralisée, soit par une mise à jour sur le serveur, soit par la mise à jour des terminaux commandée en une fois depuis le serveur. Cette répartition des éléments applicatifs permet aussi une administration à distance avec une gestion de paramètres différenciés selon les points d'acceptation ou les pays dans lesquels ils se situent.

²⁶ Lors des travaux conduits par le groupe « Veille technologique », plusieurs annonces ont également été faites pour ajouter un lecteur de cartes de paiement sur des téléphones équipés d'un clavier et disposant d'une connexion à Internet (« smartphones »), afin de leur faire jouer le rôle d'un terminal de paiement. Ce type d'équipement pourrait être dès lors apparenté à un terminal « léger ».

Encadré 8 – Principes du paiement à distance par courrier et téléphone



Les solutions de sécurité

Les terminaux de paiement classiques déployés aujourd'hui assurent plusieurs fonctions de sécurité. Il peut s'agir de contrôles réalisés « en local » par le terminal lui-même, ou « à distance », en connexion avec les serveurs d'autorisation des banques²⁷. L'exécution de ces contrôles est guidée par des règles de gestion de risques dépendant du type de carte et de l'importance de la transaction :

- en local, un terminal classique vérifie, par des dialogues cryptographiques, les éléments sécurisés inscrits sur la puce de la carte. A l'insertion de la carte, une première série de contrôles permet de s'assurer de l'authenticité de celle-ci. Ensuite, la saisie du code confidentiel (PIN) sur le clavier du terminal entraîne une série de vérifications, et notamment celle de ce code, par confrontation avec celui inscrit de manière sécurisée dans la puce de la carte. Le terminal contient également des fichiers de numéros de cartes en opposition afin de les rejeter ;
- connecté au serveur d'autorisation, le terminal peut effectuer une demande d'autorisation visant à obtenir la validation de la transaction par la banque émettrice. Les données transmises sont celles de la transaction (montant, numéro de la carte, date d'expiration, CVX, numéro d'identification du commerçant). La validation de la transaction se fonde sur un contrôle de la validité de la carte et sur la vérification éventuelle de l'existence d'une provision au compte. Pour les transactions validées, le terminal réalise le fichier de télécollecte de manière scellée, ce qui permet de s'assurer de son intégrité lorsque celui-ci est transmis en fin de journée au serveur acquéreur.

En comparaison, un terminal « léger » a, par principe, vocation à effectuer un minimum de contrôles, les autres étant alors pris en charge par le serveur. Parmi les contrôles habituellement effectués en local par un terminal classique, il est envisageable que soient réalisés sur le serveur de contrôle monétique :

- l'application des règles de gestion de risque gouvernant les contrôles à réaliser pour une carte ;

²⁷ En anglais les premiers sont appelés « off-line » et les seconds « on-line ».

- le contrôle de la validité de la clé d'authentification de la carte. Dans cette hypothèse, il serait nécessaire de protéger les données transmises sur le réseau de communication entre le terminal et le serveur de contrôle monétique ;
- le contrôle de l'inscription de la carte sur des fichiers d'opposition ;
- la confection des demandes d'autorisation et des fichiers de transactions qui sont transmis aux serveurs d'acquisition.

En revanche, la vérification du code PIN n'a pas vocation à être déportée sur le serveur de contrôle monétique.

Le terminal « léger » garde une sensibilité face aux risques de détournements (captation du code PIN ou prise de contrôle du flux, voire risque d'entrée dans le réseau). Mais la sensibilité des autres équipements est également modifiée. Le serveur de contrôle monétique devient un élément sensible dans la chaîne de transmission et de traitement des données. Il devient, par ailleurs, un équipement impliqué directement dans les opérations de gestion et de maintenance à distance des terminaux puisqu'il centralise les mises à jour de programmes à effectuer. De plus, la protection des flux de données qui sont échangés, dans un premier temps, entre le terminal « léger » et le serveur de contrôle monétique, puis entre ce même serveur de contrôle monétique et le serveur d'acquisition, devient cruciale.

En conséquence, un certain nombre de mesures de sécurité sont requises pour assurer la confidentialité, l'intégrité et la disponibilité des données :

- le serveur de contrôle monétique et le terminal « léger » doivent être protégés de façon à éviter la compromission de données ou la prise de contrôle du flux. Il est pour cela nécessaire de s'assurer de l'authenticité et de l'intégrité physique et logique de ces dispositifs ;
- les systèmes d'exploitation des équipements ainsi que les applications installées doivent être maintenus à l'état de l'art afin de garantir leur sécurité, et notamment leur intégrité ;
- les flux de données entre le terminal « léger » et le serveur de contrôle monétique doivent être protégés pour garantir l'authenticité et la confidentialité des données échangées. Les mesures déployées doivent être adaptées selon que le serveur de contrôle monétique est situé chez le commerçant ou chez son prestataire. Dans ce dernier cas, et notamment en raison de l'usage de réseaux le plus souvent ouverts²⁸, une sécurisation accrue des flux échangés est souhaitable. Par ailleurs, le terminal « léger » devant être en permanence en communication avec le serveur de contrôle monétique, il convient de s'assurer que les réseaux employés sont configurés afin de garantir la disponibilité des données échangées ;
- il en va de même pour les échanges de données entre le serveur de contrôle monétique et le serveur d'acquisition. A titre d'exemple, ceux-ci peuvent être réalisés par le chiffrement des données et par l'utilisation de réseaux privés virtuels (VPN – *Virtual private Network*) ou d'un protocole de sécurisation de type SSLv3 ou équivalent²⁹.

Par ailleurs, les exigences sécuritaires des systèmes de paiement par carte doivent être adaptées à l'architecture des terminaux « légers » afin de ne pas dégrader le niveau de protection actuel du dialogue entre la puce et le terminal et des données traitées par les dispositifs.

²⁸ Cf. Rapport annuel 2006 de l'Observatoire, Utilisation de réseaux ouverts dans l'environnement des cartes de paiement, pp. 25 à 30.

²⁹ Cf. Rapport annuel 2006 de l'Observatoire, Utilisation de réseaux ouverts dans l'environnement des cartes de paiement.

Les changements applicatifs pouvant être réalisés de manière centralisée, il devient possible de les mettre à jour dans un délai très bref, ce qui permettrait, en cas de défaillance de la sécurité, d'intervenir au plus vite.

Conclusion et propositions de recommandations

Les terminaux « légers » sont encore au stade d'étude, ce qui ne permet pas de décrire les fonctionnalités exactes dont ils disposeront. Toutefois, les pilotes en cours de préparation et l'intérêt existant autour de la gestion à distance de parcs de terminaux laissent à penser que ces nouveaux dispositifs seront amenés à se développer dans les prochaines années. Dans ce contexte, l'Observatoire s'est attaché à analyser le fonctionnement qui pourrait être celui d'un terminal « léger », et à examiner les mesures de sécurité qui pourraient être mises en œuvre.

L'Observatoire note ainsi qu'il est envisageable que la majorité des contrôles réalisés par un terminal classique lors du paiement par carte puissent être déportés sur un serveur de contrôle monétique distant, la vérification du PIN ayant toutefois vocation à s'effectuer au niveau du terminal « léger ». Celui-ci demeure donc un élément sensible de la chaîne de paiement, mais le serveur de contrôle monétique en devient également un. De plus, la protection des flux de données échangés entre le terminal « léger » et ce serveur devient cruciale.

L'Observatoire a en conséquence identifié un certain nombre de mesures de sécurité pour assurer la confidentialité, l'intégrité et la disponibilité des données sensibles du paiement par carte. Ces mesures concernent notamment la protection du serveur de contrôle monétique et celle du terminal « léger », ainsi que les flux échangés entre ces différents équipements. L'Observatoire recommande aux acteurs qui mettraient en œuvre des architectures monétiques utilisant des terminaux « légers » de veiller à appliquer de telles mesures. Il recommande par ailleurs que les exigences sécuritaires des systèmes de paiement par carte soient adaptées à l'architecture des terminaux « légers » afin de conserver le niveau de protection actuel du dialogue entre la puce et le terminal et des données traitées par les dispositifs.

3|4 État d'avancement de la migration EMV

La mise en œuvre en Europe des spécifications EMV (« Europay, Mastercard, Visa ») pour carte à puce représente un enjeu majeur dans la lutte contre la fraude transfrontalière. Elle concerne non seulement les cartes elles-mêmes, mais aussi leurs dispositifs d'acceptation (terminaux, automates de paiement et de retrait) qu'il convient de migrer aux nouvelles spécifications pour pouvoir bénéficier d'un niveau de protection égal partout en Europe. Comme il le fait depuis cinq ans de façon à mesurer l'avancement de la migration EMV, l'Observatoire a de nouveau recueilli auprès du Groupement des Cartes Bancaires « CB » et de l'EPC des statistiques relatives à cette migration en France et en Europe. Ces chiffres montrent que la migration est en cours partout en Europe, avec une progression correcte dans la plupart des pays, globalement en ligne avec l'engagement des banques européennes au sein de l'EPC d'avoir achevé cette migration d'ici à fin décembre 2010. L'Observatoire s'inquiète cependant des disparités persistantes dans la progression de la migration, qui sont susceptibles de laisser perdurer une fraude transfrontalière européenne significative.

État de la migration en France

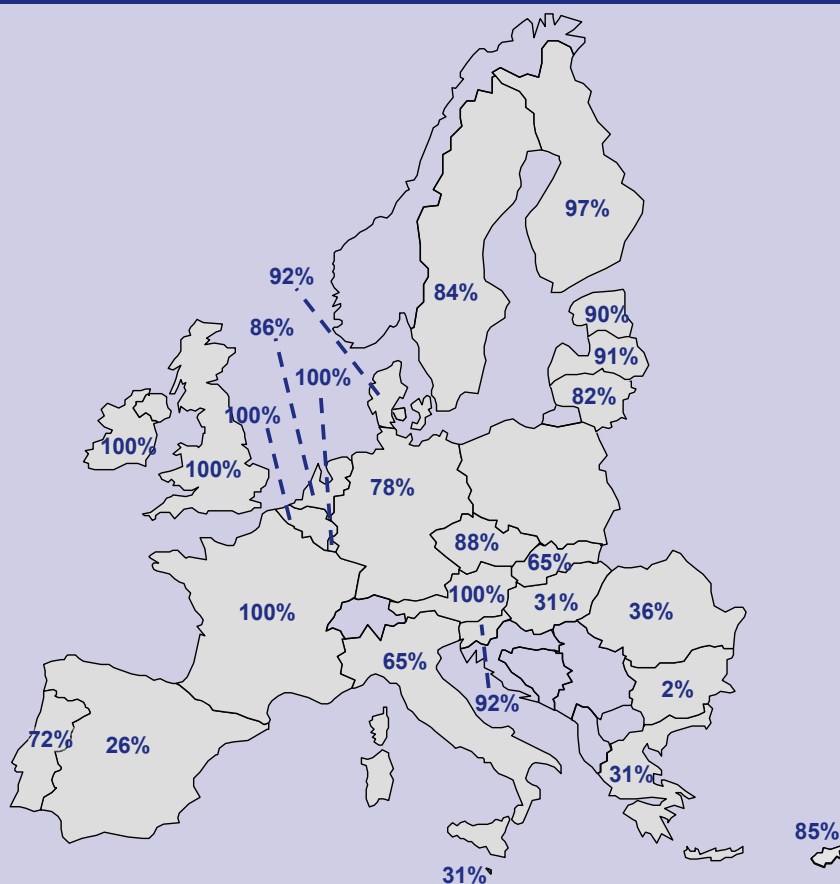
En France, la migration au standard EMV est quasiment terminée. Fin mars 2010, selon les statistiques établies par le Groupement des Cartes Bancaires « CB », 100 % des cartes « CB », 99,8 % des terminaux et automates, et 100 % des distributeurs automatiques de billets étaient

conformes aux spécifications EMV. Le 0,2 % restant de terminaux et automates, peu utilisés, seront migrés lors de leur remplacement normal.

État de la migration en Europe

Au niveau européen, selon les chiffres fournis par l'EPC et arrêtés à fin mars 2010, 69,8 % des cartes interbancaires circulant au sein des 27 États membres de l'Union européenne sont maintenant conformes à la spécification EMV (+ 2,3 points par rapport à mars 2009). Pays par pays, la situation reste contrastée (voir Encadré 9). Alors que la mise en conformité aux règles d'interopérabilité de SEPA a commencé depuis début 2008, la migration EMV de plusieurs pays est soit à peine débutée (Bulgarie), soit reste peu avancée (Espagne, Hongrie).

Encadré 9 – Déploiement des cartes EMV en Europe



Source : European Payments Council – mars 2010

Par rapport à l'an dernier, on constate une progression générale de la migration des cartes au standard EMV. Toutefois, plusieurs pays débutent à peine leur migration, comme la Bulgarie et la Pologne, ou sont peu avancés, comme l'Espagne, et la Hongrie.

Le déploiement des cartes EMV reste plus élevé dans les pays du Nord de l'Europe.

Concernant l'acquisition, la migration vers EMV progresse sensiblement : à fin mars 2010 80,0 % des terminaux de paiement (voir Encadré 10) et 94,4 % des distributeurs automatiques de billets (voir Encadré 11) sont conformes à EMV (soit une progression de 4 points pour les terminaux de paiement et de 2,4 points pour les distributeurs automatiques de billets par rapport à mars 2009). La situation reste très contrastée pays par pays, tant en taux d'équipement qu'en progression d'une année sur l'autre.

Encadré 10 – Déploiement des terminaux et automates EMV en Europe



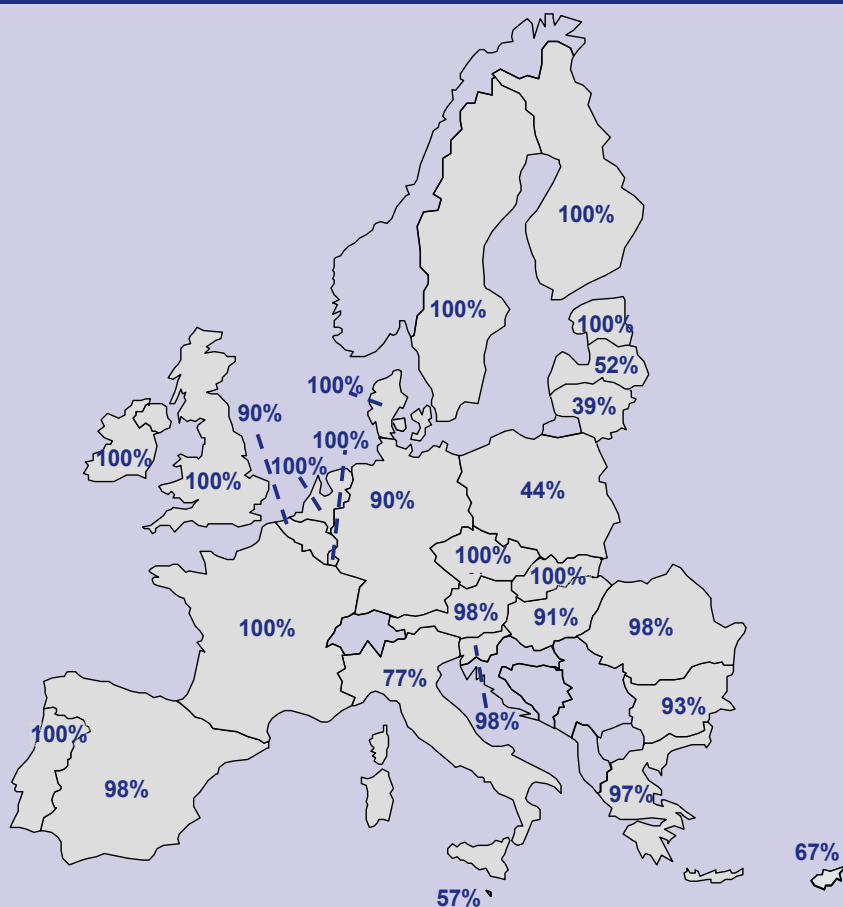
Source : European Payments Council – mars 2010

La tendance observée pour les terminaux et les automates est à l'inverse de celle constatée pour le déploiement des cartes : la migration des terminaux est globalement plus rapide dans les pays du Sud de l'Europe, qui sont les régions les plus touristiques et donc les plus susceptibles d'enregistrer des volumes élevés de transactions transfrontalières.

La situation évolue toujours peu en Allemagne par rapport à mars 2008, ce pays restant à un faible niveau d'équipement. La migration a en revanche progressé en Suède et aux Pays-Bas.

Les pays en fin de migration peuvent rencontrer des difficultés à remplacer une dernière frange de systèmes d'acceptation, qui sont peu ou très ponctuellement utilisés.

Encadré 11 – Déploiement des distributeurs de billets EMV en Europe



Source : European Payments Council – mars 2010

La progression de la migration des distributeurs de billets est plus homogène dans les différents pays européens et les taux de migration sont globalement plus élevés que pour les cartes et les terminaux. Il subsiste toutefois quelques disparités. Les pays en cours de migration de leur parc de distributeurs automatiques de billets au standard EMV ont probablement choisi de migrer en priorité les automates utilisés par les touristes et les visiteurs étrangers. L'Italie reste légèrement en deçà des niveaux de déploiement des autres grands pays mais son niveau d'équipement s'est encore amélioré depuis mars 2009.

4 | PERCEPTION PAR LES PORTEURS DE LA SÉCURITÉ DES CARTES DE PAIEMENT

Dans la continuité du sondage effectué en 2007, l'Observatoire a souhaité actualiser les données collectées relatives à la perception de la sécurité des cartes de paiement par les porteurs. Dans la lignée des recommandations effectuées par la Banque de France quant à la sécurisation des opérations sensibles en ligne, l'étude menée cette année porte une attention plus particulière à la perception de la sécurité des paiements en ligne et aux réactions liées à l'utilisation de dispositifs de sécurisation.

Dans cette perspective, l'Observatoire a fait procéder à deux études, l'une quantitative et l'autre qualitative, menées respectivement par l'institut CSA et l'institut LH2. La première a été conduite auprès d'un échantillon représentatif de 1 010 personnes âgées de 18 à 74 ans résidant en France métropolitaine, contactées par téléphone du 8 au 15 février 2010³⁰. La seconde, qui a porté plus particulièrement sur la perception de la sécurité des paiements en ligne et l'accueil porté à cinq dispositifs d'authentification non rejouable³¹, était constituée d'entretiens individuels semi-directifs réalisés avec 40 personnes âgées de 18 à 65 ans³².

4|1 Les résultats de l'étude sur la perception de la sécurité des cartes de paiement par les porteurs confirment les tendances observées en 2007

Un équipement stabilisé mais des usages qui s'intensifient, notamment pour les paiements sur Internet

Une très large majorité des personnes interrogées, 9 personnes sur 10, détient aujourd'hui au moins une carte de paiement ou de retrait. La raison principale qui motive le fait de ne pas détenir de carte est l'absence de besoin, exprimée par 5 % des Français. Mais seul 1,5 % de la population déclare ne pas posséder de carte pour des raisons de sécurité.

L'usage de la carte en France est totalement banalisé puisque 8 porteurs sur 10 l'utilisent à chaque fois que cela est possible ou presque. Par rapport à 2007, l'usage de la carte en France est en légère progression pour les paiements sur automates et chez les commerçants.

³⁰ L'échantillon a été construit selon la méthode des quotas qui portaient sur le sexe, l'âge, le statut professionnel et la profession des personnes interrogées, ainsi que sur la taille d'agglomération et la région d'habitation. Le sondage a été précédé d'une phase qualitative qui a consisté à réunir, à Paris et en province, plusieurs groupes de porteurs présentant chacun des comportements similaires en termes d'usages de leurs cartes.

³¹ Un dispositif d'authentification non rejouable associé à un moyen de paiement repose sur l'utilisation de codes à usage unique, c'est-à-dire utilisables pour la protection d'une seule transaction, permettant d'authentifier de manière renforcée un porteur ou usager légitime de ce moyen de paiement.

³² Les critères principaux qui ont servi à structurer l'échantillon sont : la fréquence des pratiques de paiement en ligne, le fait d'utiliser ou non un dispositif de sécurisation, ainsi que des paramètres assurant une bonne représentativité dans le cadre d'une étude qualitative (répartition hommes/femmes, tranches d'âge concernées, statut professionnel, usage d'Internet, localisation Paris/province). La durée de chaque entretien a été d'environ 1h15 à 1h30.

En revanche, on constate une assez forte progression de l'utilisation de la carte pour les paiements sur Internet par rapport à la précédente étude. En effet, en 2010 un Français sur deux effectue des achats en ligne avec sa carte bancaire contre 38 % en 2007.

Comme en 2007, des réticences dans l'utilisation de la carte de paiement subsistent toutefois pour les paiements à l'étranger : 34 % des voyageurs en Europe et 41 % des voyageurs hors Europe n'effectuent jamais de retrait à l'étranger. Ainsi, 13 % des porteurs de cartes voyageant à l'étranger ne l'utilisent jamais (ni pour un retrait, ni pour un paiement).

L'utilisation des cartes est perçue comme sûre par la grande majorité des porteurs

Plus des trois quarts des porteurs de cartes de paiement (77 %) considèrent que l'utilisation de la carte reste sûre, même si ce pourcentage est légèrement en baisse depuis 2007 (3 points). Un tiers des personnes interrogées considère que les cartes de paiement permettent de réaliser des achats avec le moins de risques.

Les personnes qui perçoivent la carte comme étant le moyen de paiement le plus sûr sont principalement les personnes âgées de plus de 65 ans, les retraités, les personnes ayant au moins un niveau d'études secondaires ainsi que celles vivant en couple ou voyageant en Europe.

Malgré tout, il subsiste un décalage entre l'opinion globale que les porteurs expriment au sujet de la sécurité des cartes et le sentiment ressenti en situation d'utilisation. En effet, près de 46 % des Français déclarent avoir l'impression de prendre tout de même un risque lors d'un paiement par carte.

Des paiements par carte perçus comme plus sûrs chez les commerçants en France que sur Internet ou à l'étranger

Les opérations réalisées en France sont perçues comme étant les plus sûres. En particulier, le paiement chez un commerçant en France est l'opération jugée comme étant la plus sûre, avec 94 % d'opinions en ce sens.

Les craintes concernant les paiements par courrier ou téléphone sont plus importantes en 2010 qu'en 2007 puisque seuls 25 % des porteurs, contre 32 % en 2007, pensent que payer par courrier ou téléphone est sûr. De même, la perception du risque s'est accentuée pour les paiements chez les commerçants à l'étranger : 51% des porteurs, contre 57 % en 2007, considèrent que payer chez un commerçant à l'étranger est une opération sûre.

Les paiements sur Internet sont, eux, perçus comme risqués, en France comme à l'étranger. Lorsque le site est français, seule la moitié des porteurs de carte juge les paiements sur un tel site comme étant sûrs. Cette perception du risque est nettement plus importante lorsque le site est étranger ou en langue étrangère puisque seul un détenteur de carte sur 10 perçoit ces paiements comme étant sécurisés.

De même qu'en 2007, 44 % des utilisateurs de carte ont déjà utilisé un autre moyen de paiement que la carte en raison de leur perception du risque. Pour 37 % de ces personnes, il s'agissait de paiements sur Internet.

Les réflexes de sécurité sont bien intégrés mais l'information des porteurs sur les actions à mener en cas de fraude reste à améliorer

Même si les trois quarts des utilisateurs de cartes, contre 66 % en 2007, considèrent que les établissements financiers sont les mieux placés pour améliorer la sécurité des cartes, 76 % d'entre eux pensent avoir également un rôle à jouer pour éviter les fraudes. Cette proportion tend à progresser depuis 2007 (72 %), ce qui témoigne de l'avancée de l'appropriation des réflexes de sécurité.

La majorité des porteurs de cartes prend systématiquement des précautions pour éviter les risques liés à l'utilisation de la carte. Les pratiques les plus répandues consistent en la vérification de la sécurisation du site sur Internet³³, l'adoption d'une attitude de discrétion lors de l'entrée du code PIN chez un commerçant ou la vérification du montant affiché avant de valider le paiement.

Toutefois, cette vigilance pourrait être accrue si les consommateurs étaient mieux informés sur les risques et les mesures à adopter en cas de fraude. En effet, 4 utilisateurs de carte sur 10 prêtent encore leur carte à leur entourage, même si ce comportement s'est atténué depuis 2007 (5 sur 10). Même si la proportion de personnes qui pensent être responsables en cas d'utilisation frauduleuse de leur carte si celle-ci est encore en leur possession a baissé (19 % en 2010 contre 25 % en 2007), le délai pendant lequel il est possible d'effectuer une opposition reste encore largement méconnu. 59 % des utilisateurs l'estiment à 10 jours ou moins et seuls 4 % ont été informés de l'allongement de ce délai sous certaines conditions, conformément aux dispositions prévues par la Directive européenne sur les services de paiement.

L'exposition directe ou indirecte à la fraude n'a pas d'influence significative sur les comportements des utilisateurs

L'exposition à la fraude des porteurs de carte reste du même ordre qu'en 2007 : 13 % déclarent avoir déjà été eux-mêmes victimes de fraude et 18 % ont été exposés à la fraude de manière indirecte. La principale source de fraude rapportée est liée au paiement sur Internet (27 % des cas rapportés).

L'impact de l'exposition à la fraude est assez limité quoique plus important qu'en 2007 puisque presque la moitié des victimes de fraude (45 % contre 37 % en 2007) déclarent avoir diminué l'utilisation de leur carte suite à la fraude.

Après une fraude, les utilisateurs restent tout de même confiants vis-à-vis de leur carte : 63 % des personnes exposées directement à la fraude disent que l'utilisation de leur carte est sûre, contre 77 % de manière générale. En revanche, l'exposition indirecte à la fraude n'a pas d'impact sur la perception de la sécurité des cartes.

³³ En vérifiant notamment la présence de pages chiffrées lors d'un paiement (présence du cadenas de sécurité à cet effet).

Encadré 12 – Types d'attitude en matière de sécurité des cartes

L'enquête réalisée permet d'identifier plusieurs types de comportement et d'attitude chez les utilisateurs de carte* :

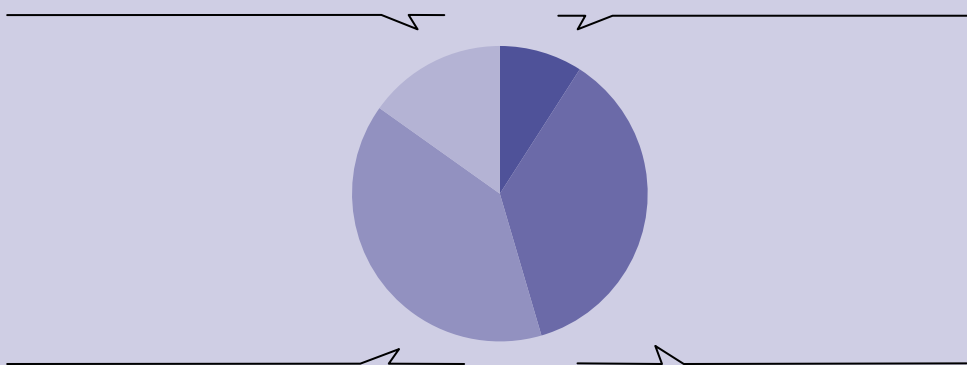
Les inquiets vigilants (15 %)

Ils paient le moins souvent possible avec leur carte quel que soit le canal. Ils perçoivent les cartes en général, comme étant risquées, voire très risquées, quel que soit le canal et ont l'impression de prendre des risques en l'utilisant. Ils n'ont pas un niveau de connaissance élevé de leur carte.

Les confiants (9 %)

Ils paient avec leur carte chaque fois que cela est possible. Ils perçoivent l'utilisation de la carte comme étant très sûre et n'ont pas du tout l'impression de prendre de risques en l'utilisant. Ils ne prennent pas beaucoup de précautions.

→ Un groupe qui est resté stable par rapport à 2007



Les résignés (36 %)

Ils utilisent moins leur carte que les autres même s'ils jugent globalement l'utilisation de la carte assez sûre. Par contre, ils ont l'impression de prendre des risques à chaque utilisation. Ils prennent moins de précautions qu'en 2007.

→ Ils représentent 36 % des utilisateurs de cartes contre 28 % en 2007.

Les avertis (39 %)

Ils paient avec leur carte chaque fois que cela est possible et jugent l'utilisation des cartes assez sûre. Ils ne ressentent pas de risques en utilisant leur carte. Pour eux, la sécurité des cartes progresse et ils prennent systématiquement un certain nombre de précautions pour éviter les fraudes.

→ Les avertis étaient 28 % en 2007, ils sont maintenant plus nombreux : 39 %.

* Cette typologie des utilisateurs de cartes a été réalisée selon la même méthode qu'en 2007. Étant donné les changements du questionnaire, seuls quatre groupes au lieu de cinq en 2007 ont pu être détectés. Trois groupes sont directement comparables à ceux obtenus en 2007 : les confiants, les avertis et les résignés. Le groupe des méfiants s'est réparti entre les deux derniers et les inquiets sont devenus plus vigilants.

4|2 Les utilisateurs des paiements en ligne présentent une sensibilité réelle au risque de fraude et accueillent de manière favorable l'implication de leur banque dans la diffusion de dispositifs de sécurisation

L'étude qualitative conduite par l'institut LH2 a permis de mettre en avant une sensibilité réelle des acheteurs aux risques de fraude et une réaction positive face à l'implication de leur banque dans leur sécurisation.

La perception de la sécurité des transactions effectuées lors des achats en ligne

Un risque de fraude perçu comme immatériel

Le risque de fraude associé au paiement sur Internet n'apparaît pas tout d'abord comme un frein majeur au développement des achats en ligne. Des considérations liées au principe même de l'achat sur Internet ou à l'image du site Internet sur lequel se fait l'achat sont des obstacles beaucoup plus puissants au paiement en ligne. En effet, ce sont davantage des craintes de ne pas être livré, de recevoir une marchandise détériorée ou bien résultant du peu de confiance qu'inspire le site du commerçant qui constituent les principaux obstacles à l'achat en ligne.

Si la fraude liée au paiement en ligne ne fait pas l'objet d'une intuition immédiate, c'est principalement parce que le risque de fraude est perçu comme immatériel. Le fait de ne pas savoir comment précisément peut advenir la fraude conduit soit à une méfiance généralisée envers l'informatique et Internet (« *J'ai l'impression qu'on peut accéder facilement à tous les ordinateurs* », « *on peut tout faire par Internet* ») soit à l'oubli du risque. Le cadenas et la mention « https » sur l'écran lors de l'achat sont souvent les seuls symboles qui rappellent la matérialité du risque de fraude encouru lors du paiement en ligne.

Une sensibilité réelle mais différenciée face au risque de fraude

Malgré tout, il existe une sensibilité réelle au risque de fraude pour tous, même si le vécu de la perception du risque est différent en fonction de l'expérience et de la personnalité des individus. Trois profils se dégagent à cet égard :

- les « craintifs », qui se répartissent sur toutes les classes d'âge de 25 à 65 ans, présentent une sensibilité forte au risque de piratage sur Internet du fait d'une approche intellectualisée de ce risque, même sans expérience positive ou négative. Pour eux, le fait de donner ses coordonnées de carte bancaire lors du paiement sur Internet constitue un véritable blocage au paiement en ligne ;
- les « prudents » évoquent la fraude sur Internet et pensent qu'il existe toujours un risque, mais ils procèdent tout de même à des achats en ligne, de manière plus ou moins régulière, y compris pour de gros montants. Il s'agit en majorité des personnes âgées de 35 à 60 ans qui effectuent des paiements en ligne de chez eux ;
- les « vigilants » sont conscients du risque de fraude mais il s'agit davantage pour eux d'une étape à franchir que d'une préoccupation permanente. Une fois la confiance venue avec la pratique et l'expérience de l'entourage, le risque de fraude n'est plus un obstacle aux achats récurrents sur Internet. Il s'agit d'une majorité de personnes de 20-25 ans, effectuant des paiements sur Internet de chez eux ou bien en mobilité hors du foyer.

Les comportements de sécurisation adoptés par les utilisateurs

La perception de l'existence d'un risque quant à la sécurité des transactions en ligne conduit les acheteurs à adopter eux-mêmes des mesures de sécurisation. Elles sont de plusieurs sortes : une attention portée à la réputation du site Internet et au fait que celui-ci soit sécurisé, la vérification de l'existence du cadenas et de la mention « https », la lecture des dispositions de sécurité du site, le fait de ne pas sauvegarder ses coordonnées bancaires sur son ordinateur, le fait de ne pas acheter en répondant à un mail reçu mais en passant par le site officiel du marchand, ou la vérification de la déconnexion de la page de paiement après que celui-ci ait été effectué.

Toutefois, les comportements adoptés par les acheteurs en ligne à l'égard de la fraude sont parfois incohérents, notamment lorsque ceux-ci n'appliquent pas de manière systématique les mesures de sécurisation qu'ils adoptent. Ainsi, ces mesures seront appliquées pour des achats de gros montant et non pour de petits achats. Si le prix est très intéressant, ils feront un achat sur un site non sécurisé.

A cet égard, il semble que la sensibilité au risque de fraude en ligne s'émousse parfois avec le temps et l'absence d'expérience négative. En effet, la confiance dans le site du commerçant ou l'expérience antérieure positive sur tel site prime sur les mesures de sécurité affichées.

L'utilisation d'un dispositif de sécurisation : un enjeu relationnel fort avec la banque

Un accueil positif de l'engagement et de l'accompagnement des banques

Les dispositifs de sécurisation des paiements en ligne proposés par les banques sont toujours bien accueillis par les acheteurs, qu'ils pratiquent beaucoup ou peu les paiements sur Internet. En particulier, l'implication des banques dans la diffusion de ces dispositifs est perçue comme un gage de l'efficacité et de la sécurité des solutions proposées.

Plus précisément, les acheteurs sont particulièrement réceptifs à une démarche globale, massive des banques, démarche qui véhicule alors plusieurs conséquences :

- au plan symbolique : en s'impliquant, les banques contribuent à une moralisation du commerce en ligne. En effet, les utilisateurs n'imaginent pas qu'elles mettent en place un dispositif de sécurisation auprès de sites peu fiables ;
- au plan psychologique : la mise en place de dispositifs de sécurisation entre dans le cadre d'une relation privilégiée entre l'internaute et sa banque. Le fait que cette dernière s'engage à offrir plus de tranquillité d'esprit et agisse dans l'intérêt de ses clients renforce le lien qui existe entre l'utilisateur du paiement en ligne et sa banque ;
- au plan financier : le déploiement de dispositifs techniques de sécurisation a priori et de mécanismes d'assurance a posteriori garantit une tranquillité d'esprit qu'envisage positivement l'acheteur en ligne.

Les facteurs de réussite d'une diffusion des dispositifs de sécurisation

L'étude a permis de relever que la réussite de la généralisation de dispositifs de sécurisation des transactions en ligne dépend d'un certain nombre de conditions.

Tout d'abord, les dispositifs doivent être adaptés et compatibles avec les différents types de comportement ou d'usage. Si de tels dispositifs devraient encourager les « craintifs » à passer à l'acte et accompagner les « prudents » dans leur appropriation du paiement en ligne, il faudrait encore qu'ils soient adaptés pour que les « vigilants », qui sont davantage familiarisés au paiement en ligne, les utilisent fréquemment. Les dispositifs proposés devraient par conséquent être adaptés à chaque type d'utilisateur de manière que chacun puisse se l'approprier et en retirer le bénéfice attendu de son utilisation.

Ensuite, le déploiement de dispositifs de sécurisation des transactions en ligne doit être accompagné d'une communication appropriée de la part des banques. Les démarches des banques dans ce domaine sont perçues positivement et très largement appréciées, à condition que les utilisateurs bénéficient d'un accompagnement lors de la diffusion des dispositifs de sécurisation.

4|3 Les réactions face à l'utilisation de dispositifs de sécurisation des paiements en ligne sont toujours positives

Des réactions positives

Les dispositifs d'authentification non rejouable

Cinq dispositifs³⁴ d'authentification non rejouable utilisables sur un site Internet marchand ont été portés à l'appréciation des sujets de l'étude qualitative.

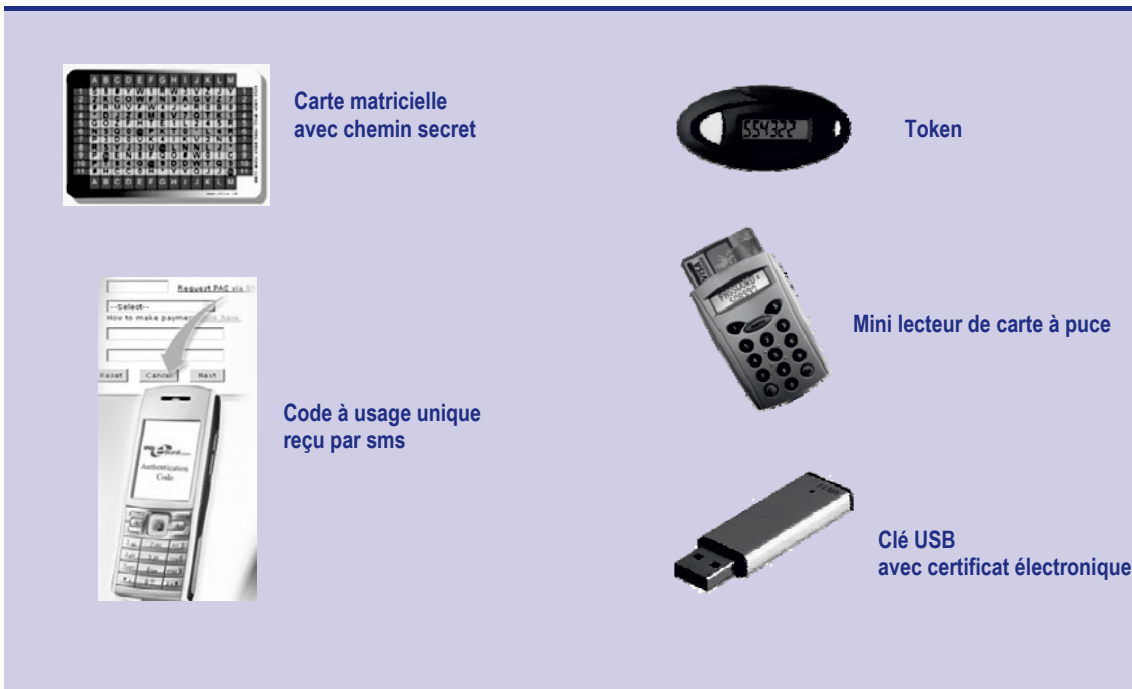
Quatre dispositifs ont pour objet de générer un code à usage unique devant être renseigné sur Internet lors du paiement :

- la carte matricielle avec chemin secret : le code à usage unique est produit à partir de la saisie de codes obtenus sur la carte selon un chemin connu seulement de l'utilisateur ;
- le « Token » : le code à usage unique est généré par un algorithme placé dans un petit appareil électronique suite à une pression sur un bouton ;
- le code à usage unique reçu par SMS ;
- le mini lecteur de carte à puce : le code à usage unique s'affiche sur l'écran du lecteur après insertion de la carte bancaire du porteur et saisie de son code PIN.

Le cinquième dispositif d'authentification non rejouable présenté est la clé USB avec certificat électronique que l'internaute doit connecter à son ordinateur lors du paiement avant entrée du code PIN de la clé, nécessaire à l'authentification.

³⁴ Dispositifs fournis pour les besoins de l'enquête par les sociétés Elca, Vasco et Xiring (maintenant Gemalto).

Encadré 13 - Dispositifs d'authentification non rejouable



Un accueil positif des dispositifs de sécurisation

La diffusion de dispositifs de sécurisation des transactions en ligne est perçue comme le vecteur d'une tranquillité d'esprit très appréciable. Les utilisateurs du paiement en ligne font confiance aux banques pour mettre en place des dispositifs fiables dans la mesure où cela relève de leur compétence et que cela paraît légitime. En particulier, le fait de devoir passer par le site de la banque lors de l'authentification est toujours très bien vécu.

L'allongement du temps de réalisation de la transaction sur Internet, du fait de l'étape supplémentaire imposée par l'authentification du paiement, ne semble pas poser de problème en soi.

Les critères des réactions

Les réactions positives des utilisateurs varient en fonction de trois types de caractéristiques des dispositifs présentés :

- l'adéquation avec le mode de vie de l'utilisateur et les pratiques de paiement en ligne actuelles : le dispositif (lecteur, carte, clé...) va incarner, matérialiser un risque de fraude généralement perçu comme immatériel. Il sera d'autant mieux reçu qu'il sera en accord avec le mode de vie et les sensibilités de son détenteur (mobilité ou pas) et sa perception du paiement en ligne (très ou peu risqué) ;
- la familiarité et la facilité d'usage : l'utilisation du dispositif n'est pas pensée par rapport à un temps supplémentaire de mise en œuvre mais par rapport à la plus ou moins grande facilité d'usage, au risque d'erreur qui pourrait lui être associé et à la facilité de conservation hors des actes d'achat ;
- la fiabilité et la sécurité : une attention toute particulière est portée par les utilisateurs au risque de panne, de dysfonctionnement, de perte ou de vol du dispositif.

Des préférences différentes selon les profils

Si aucun dispositif n'est rejeté en soi, les réactions varient en fonction de l'expérience en matière de paiements en ligne.

Les choix varient en fonction du profil de l'acheteur, les plus gros acheteurs privilégiant la simplicité et la facilité d'utilisation en mobilité, tandis que les petits acheteurs privilégient l'image de sécurité mise en scène et le rappel de l'acte de paiement par carte en magasin.

La carte matricielle avec chemin secret trouve des adeptes dans tous les profils, sans une dominance particulière. Les utilisateurs perçoivent un double avantage concernant ce dispositif : la fiabilité de par la nature du support et la sécurisation du fait de l'application d'un chemin secret. En revanche, la carte matricielle n'est souvent pas perçue comme assez moderne pour que les utilisateurs se l'approprient conformément à leur mode de vie.

Les « craintifs »

Les « craintifs », dont la sensibilité élevée au risque de fraude en ligne constitue un obstacle au paiement sur Internet, marquent une préférence relative pour le lecteur de cartes à puce qui rappelle la situation de paiement en magasin. Il est associé aux TPE des commerçants, ce qui explique une attention focalisée sur le plus gros des deux modèles présentés.

Cet objet familier inspire confiance du fait de sa simplicité d'utilisation et des gages de sécurité qu'il apporte avec la saisie du code PIN. Loin d'être lié à la carte bancaire, ce dispositif possède un aspect familial et on l'imagine ancré dans le foyer, à la maison, à proximité de l'ordinateur. Ce type de dispositif est le plus proche des pratiques de paiement envisagées par cette catégorie d'utilisateurs.

Les « prudents »

Les « prudents » quant à eux, qui présentent une sensibilité importante au risque de fraude, sans pour autant que cela soit un obstacle à la pratique de paiements plus ou moins réguliers en ligne, avouent une préférence pour le Token et l'envoi de codes à usage unique par SMS, à la fois pour leur simplicité d'utilisation et en tant que signe du passage à une utilisation en mobilité.

Le code à usage unique (« One Time Password » – OTP) reçu par SMS est un dispositif souvent déjà connu et expérimenté par les sujets de l'étude. L'aisance dans l'utilisation manifestée par ceux-ci résulte du fait que le téléphone portable est un objet familier, que l'on possède toujours avec soi et donc que la génération du code à usage unique ne nécessite pas un objet supplémentaire.

Le sentiment de sécurité associé à l'utilisation de ce dispositif lors du paiement est important du fait, d'une part de l'existence du code à usage unique et, d'autre part, du caractère personnel de l'objet utilisé.

Les « vigilants »

Les « vigilants » enfin, pour lesquels la pratique courante du paiement en ligne de chez soi ou en mobilité a atténué le sentiment de risque de fraude lors du paiement, affichent une

préférence pour le Token et la clé USB avec certificat électronique, tout en exprimant parfois des attentes d'une dématérialisation du dispositif.

Du fait de l'absence de code secret à mémoriser, le Token est un dispositif présentant une grande simplicité d'utilisation. Le code à usage unique est en effet généré uniquement en pressant un bouton présent sur le dispositif. De plus, le Token est associé spontanément par les utilisateurs à la mobilité, ce qui caractérise les pratiques de paiement des « vigilants ». Le fait que l'objet puisse être porté dans la poche ou en porte-clés rend effectivement son transport aisé. Enfin, l'existence d'un code à usage unique utilisable lors du paiement apparaît comme une garantie suffisante de la sécurisation des transactions en ligne.

La clé USB, quant à elle, est perçue comme un objet à la fois familier et moderne. L'habitude de sa manipulation dans la vie quotidienne engendre une appropriation immédiate par les internautes et une utilisation intuitive de l'outil de sécurisation des transactions en ligne. De plus, elle est associée aux instruments de nouvelle technologie, comme la clé de communication 3G.

Cet outil procure un sentiment de sécurisation fort émanant, d'une part de l'ensemble du dispositif (certificat électronique, caractère personnel de la clé USB) et, d'autre part, de l'entrée d'un code PIN spécifique à la clé USB pour générer le code à usage unique utilisé lors du paiement sur Internet. Le fait que cet objet puisse être utilisé à la fois chez soi et en mobilité explique qu'il soit le plus en conformité avec les pratiques de paiement en ligne des « vigilants ».

Des impacts nuancés sur les comportements de paiement

La diffusion de dispositifs de sécurisation des paiements en ligne aurait un impact sur les comportements de paiement de l'ensemble des porteurs mais celui-ci serait différencié selon les profils d'acheteurs.

Les « craintifs » devraient passer à l'acte de paiement sur Internet

Les « craintifs », qui se caractérisent par le fait que leur sensibilité élevée au risque de fraude constitue un obstacle au paiement sur Internet, déclarent le plus souvent que la mise en place de dispositifs de sécurisation des transactions en ligne devrait les conduire à passer à l'acte.

Toutefois cette réaction doit être nuancée. Certains vont passer immédiatement à l'acte en raison d'un sentiment de protection de leur banque et d'une commodité accrue du paiement par carte par rapport à d'autres moyens (envoi de chèque).

D'autres paraissent encore hésitants : ils seraient évidemment rassurés du fait de l'existence d'une garantie de sécurité lors du paiement sur Internet mais cela ne se manifesterait par une pratique effective du paiement en ligne que quelques mois ou années plus tard selon leurs propres déclarations.

Les « prudents » sont les plus sensibles à l'engagement des banques

Les « prudents », qui pratiquent le paiement sur Internet tout en ayant une sensibilité élevée au risque de fraude, apparaissent comme les plus sensibles à l'engagement des banques à leurs côtés et approuvent cette démarche d'accompagnement et d'engagement auprès des clients.

Si les effets concrets restent difficilement quantifiables, certains expriment clairement qu'ils pourraient augmenter le nombre d'achats, de sites fréquentés ou le montant de leurs achats, du fait de la tranquillité d'esprit renforcée par l'utilisation de dispositifs de sécurisation des transactions en ligne.

D'autres restent prudents et ne pensent pas se précipiter, leur comportement restant conditionné par la confiance qu'ils ont en Internet ou par l'image des sites marchands. Malgré tout, ils n'envisagent en aucun cas de diminuer leur pratique actuelle de paiement en ligne.

Les « vigilants » anticipent « plus de sérénité » mais aussi « plus de contraintes »

Les « vigilants », tout en pratiquant déjà beaucoup les achats sur Internet, apprécient la démarche des banques qui devrait leur apporter « plus de sérénité » quant aux préoccupations de sécurité des transactions.

Pour certains d'entre eux, cela n'apporterait pas de changements significatifs dans leur comportement d'achat sur Internet. Ceci peut s'expliquer par le fait qu'ils réalisent déjà beaucoup d'achats actuellement.

Pour d'autres en revanche, une meilleure sécurité des transactions en ligne aurait pour conséquence une fréquentation plus large de sites marchands et potentiellement un accroissement des achats sur Internet.

Une préférence générale pour l'efficacité perçue plutôt que pour la facilité d'utilisation

Les résultats de l'étude quantitative permettent de mieux préciser et de chiffrer les réactions dans la perception et dans le comportement des utilisateurs face à l'introduction de mesures de sécurisation des transactions en ligne. Si le périmètre de cette étude est légèrement différent de celui de l'étude qualitative (seuls quatre dispositifs sont étudiés : le mini lecteur de carte, le code à usage unique envoyé par SMS, la saisie de la date de naissance lors du paiement et la réponse à une question), il permet néanmoins de quantifier les tendances perçues lors des entretiens.

	Facilité d'utilisation	Efficacité perçue	Souhait d'utilisation
Saisie de la date de naissance	90 %	35 %	45 %
Réponse à une question	85 %	54 %	54 %
Saisie d'un code unique reçu sur le téléphone mobile	71 %	70 %	64 %
Saisie d'un code unique généré par un mini-lecteur	60 %	76 %	69 %

▲ Tableau 9 – **Les solutions d'authentification proposées par les banques : des perceptions contrastées**
(en pourcentage des payeurs par carte sur Internet)

Les chiffres ci-dessus mettent en évidence une préférence générale pour l'efficacité perçue des dispositifs en termes de sécurité plutôt que pour leur facilité d'utilisation. En effet, le souhait d'utilisation d'une des quatre solutions de sécurisation augmente à mesure que l'efficacité perçue des dispositifs s'accroît elle aussi. Les Français semblent prêts à supporter quelques contraintes d'utilisation à condition que le dispositif qu'ils utilisent lors du paiement en ligne leur paraisse efficace.

Encadré 14 – Conseils de prudence à l’usage des porteurs

Votre comportement concourt directement à la sécurité de l’utilisation de votre carte. Veillez à respecter les conseils élémentaires de prudence qui suivent afin de protéger vos transactions.

Soyez responsables

- Votre carte est strictement personnelle : ne la prêtez à personne, même pas à vos proches.
- Vérifiez régulièrement qu’elle est en votre possession.
- Si votre carte comporte un code confidentiel, gardez-le secret. Ne le communiquez à personne. Apprenez-le par cœur, évitez de le noter et surtout ne le rangez jamais avec votre carte.
- Lorsque vous composez votre code confidentiel, veillez à le faire à l’abri des regards indiscrets. N’hésitez pas en particulier à cacher le clavier du terminal ou du distributeur de votre autre main.
- Vérifiez régulièrement et attentivement vos relevés de compte.

Soyez attentifs

Lors des paiements chez un commerçant :

- Vérifiez l’utilisation qui est faite de votre carte par le commerçant. Ne la quittez pas des yeux.
- Pensez à vérifier le montant affiché par le terminal avant de valider la transaction.

Lors des retraits sur les distributeurs de billets :

- Vérifiez l’aspect extérieur du distributeur, évitez si possible ceux qui vous paraîtraient avoir été altérés.
- Suivez exclusivement les consignes indiquées à l’écran du distributeur : ne vous laissez pas distraire par des inconnus, même proposant leur aide.
- Mettez immédiatement en opposition votre carte si elle a été avalée par l’automate et que vous ne pouvez pas la récupérer immédiatement au guichet de l’agence.

Lors des paiements sur Internet :

- Protégez votre numéro de carte : ne le stockez pas sur votre ordinateur, ne l’envoyez pas par simple courriel et vérifiez la sécurisation du site du commerçant (cadenas en bas de la fenêtre, adresse commençant par « https », etc.).
- Assurez-vous du sérieux du commerçant, vérifiez que vous êtes bien sur le bon site, lisez attentivement les conditions générales de vente.
- Protégez votre ordinateur, en activant les mises à jour de sécurité proposées par les éditeurs de logiciel (en règle générale gratuites) et en l’équipant d’un antivirus et d’un pare-feu.

Lors de vos déplacements à l’étranger :

- Renseignez-vous sur les précautions à prendre et contactez l’établissement émetteur de votre carte avant votre départ, afin notamment de connaître les mécanismes de protection des cartes qui peuvent être mis en œuvre.
- Pensez à vous munir des numéros internationaux de mise en opposition de votre carte.

Sachez réagir

Vous avez perdu ou on vous a volé votre carte :

- Faites immédiatement opposition en appelant le numéro que vous a communiqué l’établissement émetteur de la carte. Pensez à le faire pour toutes vos cartes perdues ou volées.
- En cas de vol, déposez également plainte auprès de la police ou de la gendarmerie au plus vite.

En faisant opposition sans tarder, vous bénéficierez des dispositions plafonnant les débits frauduleux, au pire des cas, à 150 euros. Si vous ne réagissez pas rapidement, vous risquez de supporter l’intégralité des débits frauduleux précédant la mise en opposition. A partir de la mise en opposition, votre responsabilité ne peut plus être engagée.

Vous constatez des anomalies sur votre relevé de compte, alors que votre carte est toujours en votre possession :

Sauf en cas de négligence grave de votre part (par exemple, vous avez laissé à la vue d’un tiers le numéro et/ou le code confidentiel de votre carte et celui-ci en a fait usage sans vous prévenir) ou en cas de non-respect intentionnel de vos obligations contractuelles en matière de sécurité (par exemple, vous avez commis l’imprudence de communiquer à un proche le numéro et/ou le code confidentiel de votre carte et celui-ci en a fait usage sans vous prévenir), il faut déposer une réclamation auprès de l’établissement émetteur de la carte, dès que possible et dans un délai fixé par la loi, de 13 mois à compter de la date de débit de l’opération contestée. Dans ces conditions, votre responsabilité ne peut être engagée. Les sommes contestées doivent alors vous être immédiatement remboursées sans frais. Attention, lorsque le détournement a lieu dans un pays non européen, le délai de contestation est ramené à 70 jours à compter de la date de débit de l’opération contestée. Ce délai peut éventuellement être prolongé par votre établissement émetteur sans pouvoir dépasser 120 jours.

Bien entendu, en cas d’agissement frauduleux de votre part, les dispositions protectrices de la loi ne trouveront pas à s’appliquer et vous resterez tenu des sommes débitées avant comme après l’opposition ainsi que des éventuels autres frais engendrés par ces opérations (par exemple, en cas d’insuffisance de provision).

ANNEXE A | PROTECTION DU TITULAIRE D'UNE CARTE EN CAS DE PAIEMENT NON AUTORISÉ

L'ordonnance de transposition de la directive concernant les services de paiement au sein du marché intérieur, entrée en vigueur le 1^{er} novembre 2009, a modifié les règles relatives à la responsabilité du titulaire d'une carte de paiement.

La charge de la preuve incombe au prestataire de services de paiement. Ainsi, lorsqu'un client nie avoir autorisé une opération, il incombe à son prestataire de services de paiement de prouver que l'opération en question a été authentifiée, dûment enregistrée et comptabilisée et qu'elle n'a pas été affectée par une déficience technique ou autre. La loi encadre désormais strictement les conventions de preuve puisqu'elle prévoit que l'utilisation de l'instrument telle qu'enregistrée par le prestataire de services de paiement ne suffit pas nécessairement en tant que telle à prouver que l'opération a été autorisée par le payeur ou que celui-ci n'a pas satisfait par négligence grave aux obligations lui incombant en la matière.

Il convient toutefois de distinguer si l'opération de paiement contestée est effectuée ou non sur le territoire de la République française ou au sein de l'Espace économique européen afin de déterminer l'étendue de la responsabilité du titulaire de la carte.

Opérations nationales ou intra-communautaires

Les opérations de paiement concernées sont les opérations effectuées en euros ou en francs CFP sur le territoire de la République française¹. Sont également concernées les opérations effectuées avec une carte de paiement dont l'émetteur est situé en France métropolitaine, dans les départements d'outre-mer, à Saint-Martin ou à Saint-Barthélemy, au profit d'un bénéficiaire dont le prestataire de services de paiement est situé dans un autre État partie à l'accord sur l'EEE (UE + Lichtenstein, Norvège et Islande), en euros ou dans la devise nationale d'un de ces États.

Concernant les opérations non autorisées, c'est-à-dire en pratique les cas de perte, vol ou détournement (y compris par utilisation frauduleuse à distance ou contrefaçon) de l'instrument de paiement, le titulaire de la carte devra contester, auprès de son prestataire dans un délai de 13 mois suivant la date de débit de son compte, avoir autorisé l'opération de paiement. Son prestataire devra alors rembourser immédiatement, au titulaire de la carte, l'opération non autorisée et, le cas échéant, rétablir le compte débité dans l'état dans lequel il se serait trouvé si l'opération non autorisée n'avait pas eu lieu. Une indemnisation complémentaire pourra aussi éventuellement être versée. Nonobstant l'extension du délai maximal de contestation à 13 mois, le porteur devra, lorsqu'il a connaissance du vol, de la perte, du détournement ou de toute utilisation non autorisée de son instrument de paiement, en informer sans tarder son prestataire de services de paiement.

¹ L'ordonnance d'extension à la Nouvelle-Calédonie, à la Polynésie française et aux îles Wallis et Futuna des dispositions de l'ordonnance de transposition entre en vigueur le 8 juillet 2010.

Une dérogation à ces règles de remboursement est cependant prévue pour les opérations de paiement réalisées en utilisant un dispositif de sécurité personnalisé, par exemple la frappe d'un code secret.

Avant information aux fins de blocage de la carte

Avant « opposition »², le payeur pourra supporter, à concurrence de 150 euros, les pertes liées à toute opération de paiement non autorisée en cas de perte ou de vol de la carte si l'opération est effectuée avec l'utilisation du dispositif personnalisé de sécurité. En revanche, si l'opération est effectuée sans l'utilisation du dispositif personnalisé de sécurité, le titulaire de la carte ne voit pas sa responsabilité engagée.

La responsabilité du titulaire de la carte n'est pas non plus engagée si l'opération de paiement non autorisée a été effectuée en détournant à son insu l'instrument de paiement ou les données qui lui sont liées. Elle n'est pas plus engagée en cas de contrefaçon de la carte si elle était en possession de son titulaire au moment où l'opération non autorisée a été réalisée.

En revanche, le titulaire de la carte supporte toutes les pertes occasionnées par des opérations de paiement non autorisées si ces pertes résultent d'un agissement frauduleux de sa part ou s'il n'a pas satisfait intentionnellement ou par négligence grave à ses obligations de sécurité, d'utilisation ou de blocage de sa carte, convenues avec son prestataire de services de paiement.

Enfin, si le prestataire de services de paiement émetteur de la carte ne fournit pas de moyens appropriés permettant la mise en opposition de la carte, le client ne supporte aucune conséquence financière, sauf à avoir agi de manière frauduleuse.

Après information aux fins de blocage de la carte

Après mise en opposition de la carte, le payeur ne supporte aucune conséquence financière résultant de l'utilisation de la carte ou de l'utilisation détournée des données qui lui sont liées.

Là encore, les agissements frauduleux du titulaire de la carte le privent de toute protection et il demeure responsable des pertes liées à l'utilisation de sa carte.

L'information aux fins de blocage peut être effectuée auprès du prestataire de services de paiement ou auprès d'une entité que ce dernier aura indiquée à son client, suivant les cas, dans le contrat de services de paiement ou dans la convention de compte de dépôt.

Lorsque le titulaire de la carte a informé son prestataire de services de paiement de la perte, du vol, du détournement ou de la contrefaçon de sa carte, ce dernier lui fournit sur demande et pendant 18 mois, les éléments lui permettant de prouver qu'il a procédé à cette information.

Opérations extra européennes

La directive sur les services de paiement n'est applicable qu'aux opérations intra-communautaires. Cependant la législation française existant avant l'adoption de cette directive protégeait les titulaires de cartes sans distinction de la localisation du bénéficiaire de l'opération non autorisée. Il a été décidé de maintenir une protection équivalente à celle à

² La loi utilise désormais le terme « information aux fins de blocage de l'instrument de paiement ».

laquelle le client avait auparavant droit. A cette fin, les règles applicables aux opérations nationales ou intra-communautaires sont applicables avec des adaptations.

Ainsi, les opérations de paiement concernées par ces adaptations sont les opérations effectuées avec une carte de paiement dont l'émetteur est situé en France métropolitaine, dans les départements d'outre-mer, à Saint-Martin ou à Saint-Barthélemy, au profit d'un bénéficiaire dont le prestataire de services de paiement est situé dans un État non européen³, quelle que soit la devise dans laquelle l'opération est réalisée. Sont également concernées les opérations effectuées avec une carte dont l'émetteur est situé à Saint-Pierre-et-Miquelon, à Mayotte, en Nouvelle-Calédonie, en Polynésie française ou à Wallis et Futuna, au profit d'un bénéficiaire dont le prestataire est situé dans un État autre que la République française, quelle que soit la devise utilisée.

Dans ces cas, le plafond de 150 euros trouve à s'appliquer pour les opérations non autorisées en cas de perte ou de vol de la carte même si l'opération a été réalisée sans utilisation du dispositif personnalisé de sécurité.

Par ailleurs, le délai maximal de contestation de l'opération est ramené à 70 jours et conventionnellement étendu à 120 jours. En revanche, le remboursement immédiat de l'opération non autorisée est étendu.

³ qui n'est pas partie à l'accord sur l'EEE (UE + Lichtenstein, Norvège et Islande).

ANNEXE B | MISSIONS ET ORGANISATION DE L'OBSERVATOIRE

Le décret n° 2002-709 du 2 mai 2002 pris pour l'application de l'article L. 141-4 du Code monétaire et financier relatif à l'Observatoire de la sécurité des cartes de paiement, modifié par le décret n° 2009-654 du 9 juin 2009, a précisé les missions, la composition et les modalités de fonctionnement de l'Observatoire.¹

Cartes concernées

Il est généralement admis que constitue une carte de paiement toute carte émise par un prestataire de services de paiement permettant à son titulaire de retirer ou de transférer des fonds².

En conséquence, les compétences de l'Observatoire concernent les cartes émises par les établissements de crédit ou par les institutions assimilées et dont les fonctions sont le retrait ou le transfert de fonds. Elles ne couvrent pas les cartes monoprestataires bénéficiant d'une dérogation au monopole bancaire par l'article L. 511-7 I. 5 du Code monétaire et financier. Ces cartes, parfois appelées « cartes purement privatives », sont émises par une seule entreprise et acceptées en paiement par elle-même ou par un nombre limité d'accepteurs ayant noué avec elle un accord de franchise commerciale.

Le marché français compte de nombreuses offres en matière de cartes de paiement qui relèvent des compétences de l'Observatoire. Parmi celles-ci, on distingue généralement les cartes dont le schéma d'acceptation des paiements et des retraits repose sur :

- un nombre réduit d'établissements de crédit émetteurs et acquéreurs (cartes généralement qualifiées de « privatives ») ;
- un nombre élevé d'établissements de crédit émetteurs et acquéreurs (cartes généralement qualifiées d'« interbancaires »).

Ces cartes peuvent offrir des fonctions diverses qui conduisent à la typologie fonctionnelle suivante en matière de cartes de paiement :

- les cartes de débit sont des cartes associées à un compte de dépôt de fonds permettant à son titulaire d'effectuer des retraits ou des paiements qui seront débités selon un délai fixé par le contrat de délivrance de la carte. Ce débit peut être immédiat (retrait ou paiement) ou différé (paiement) ;
- les cartes de crédit sont adossées à une ligne de crédit, avec un taux et un plafond négociés avec le client, et permettent d'effectuer des paiements et/ou des retraits d'espèces. Elles permettent à leur titulaire de régler l'émetteur à l'issue d'un certain délai (supérieur à 40 jours en France). L'accepteur est réglé directement par l'émetteur sans délai particulier lié au crédit ;
- les cartes nationales permettent exclusivement d'effectuer des paiements ou des retraits auprès d'accepteurs établis sur le territoire français ;

¹ Les dispositions réglementaires relatives à l'Observatoire figurent aux articles R. 141-1, R. 141-2 et R. 142-22 à R. 142-27 du Code monétaire et financier.

² D'après l'article L. 132-1 du Code monétaire et financier dans sa rédaction antérieure au 1^{er} novembre 2009.

- les cartes internationales permettent d'effectuer des paiements et des retraits dans tous les points d'acceptation, nationaux ou internationaux, de la marque ou d'émetteurs partenaires avec lesquels le système de carte a signé des accords ;
- les porte-monnaie électroniques sont des cartes sur lesquelles sont stockées des unités de monnaie électronique. Aux termes de l'article 1 du règlement CRBF n° 2002-13, « une unité de monnaie électronique constitue un titre de créance incorporé dans un instrument électronique et accepté comme moyen de paiement, au sens de l'article L. 311-3 du Code monétaire et financier, par des tiers autres que l'émetteur. La monnaie électronique est émise contre la remise de fonds. Elle ne peut être émise pour une valeur supérieure à celle des fonds reçus en contrepartie ».

Attributions

Conformément aux articles L. 141-4 et R. 141-1 du Code monétaire et financier, les attributions de l'Observatoire de la sécurité des cartes de paiement sont de trois ordres :

- il suit la mise en œuvre des mesures adoptées par les émetteurs et les commerçants pour renforcer la sécurité des cartes de paiement. Il se tient informé des principes adoptés en matière de sécurité ainsi que des principales évolutions ;
- il est chargé d'établir des statistiques en matière de fraude. A cette fin, les émetteurs de cartes de paiement adressent au secrétariat de l'Observatoire les informations nécessaires à l'établissement de ces statistiques. L'Observatoire émet des recommandations afin d'harmoniser les modalités de calcul de la fraude sur les différents types de carte de paiement ;
- il assure une veille technologique en matière de cartes de paiement, avec pour objet de proposer des moyens de lutter contre les atteintes d'ordre technologique à la sécurité des cartes de paiement. A cette fin, il collecte les informations disponibles de nature à renforcer la sécurité des cartes de paiement et les met à la disposition de ses membres. Il organise un échange d'informations entre ses membres dans le respect de la confidentialité de certaines informations.

En outre, le ministre chargé de l'économie et des finances peut, aux termes de l'article R. 141-2 du Code monétaire et financier, saisir pour avis l'Observatoire en lui impartissant un délai de réponse. Les avis peuvent être rendus publics par le ministre.

Composition

L'article R. 142-22 du Code monétaire et financier détermine la composition de l'Observatoire. Conformément à ce texte, l'Observatoire comprend :

- un député et un sénateur ;
- huit représentants des administrations ;
- le gouverneur de la Banque de France ou son représentant ;
- le secrétaire général de l'Autorité de contrôle prudentiel ou son représentant ;
- dix représentants des émetteurs de cartes de paiement, notamment de cartes bancaires, de cartes privatives et de porte-monnaie électroniques ;
- cinq représentants du collège consommateurs du Conseil National de la Consommation ;
- cinq représentants des commerçants issus notamment du commerce de détail, de la grande distribution, de la vente à distance et du commerce électronique ;

- trois personnalités qualifiées en raison de leurs compétences.

La liste nominative des membres de l'Observatoire figure en annexe C.

Les membres de l'Observatoire autres que ceux représentant l'État, le gouverneur de la Banque de France et le secrétaire général de l'Autorité de contrôle prudentiel sont nommés pour trois ans. Leur mandat est renouvelable.

Le président est désigné parmi ces membres par le ministre chargé de l'économie et des finances. Son mandat est de trois ans, renouvelable. Monsieur Christian NOYER, Gouverneur de la Banque de France, assure cette fonction depuis le 17 novembre 2003.

Modalités de fonctionnement

Conformément au décret du 2 mai 2002 modifié par le décret n° 2009-654 du 9 juin 2009³, l'Observatoire se réunit sur convocation de son président, au moins deux fois par an. Les séances ne sont pas publiques. Les mesures proposées au sein de l'Observatoire sont adoptées si une majorité absolue est constituée. Chaque membre dispose d'une voix ; en cas de partage des votes, le président dispose d'une voix prépondérante. L'Observatoire a adopté en 2003 un règlement intérieur qui précise les conditions de son fonctionnement.

Le secrétariat de l'Observatoire, assuré par la Banque de France, est chargé de l'organisation et du suivi des séances, de la centralisation des informations nécessaires à l'établissement des statistiques de la fraude sur les cartes de paiement, de la collecte et de la mise à disposition des membres des informations nécessaires au suivi des mesures de sécurité adoptées et à la veille technologique en matière de cartes de paiement. Le secrétariat prépare également le rapport annuel de l'Observatoire, remis au début de chaque année au ministre chargé de l'économie et des finances et transmis au Parlement.

Des groupes de travail ou d'étude peuvent être constitués par l'Observatoire, notamment lorsque le ministre chargé de l'économie et des finances le saisit pour avis. L'Observatoire fixe à la majorité absolue de ses membres le mandat et la composition de ces groupes de travail qui doivent rendre compte de leurs travaux à chaque séance. Les groupes de travail ou d'étude peuvent entendre toute personne susceptible de leur apporter des précisions utiles à l'accomplissement de leur mandat. Dans ce cadre, l'Observatoire a constitué deux groupes de travail chargés, l'un d'harmoniser et d'établir des statistiques en matière de fraude, l'autre d'assurer une veille technologique relative aux cartes de paiement.

Étant donné la sensibilité des données échangées, les membres de l'Observatoire et son secrétariat sont tenus de conserver confidentielles les informations qui sont portées à leur connaissance dans le cadre de leurs fonctions. A cette fin, l'Observatoire a inscrit dans son règlement intérieur l'obligation incombant aux membres de s'engager auprès du président à veiller strictement au caractère confidentiel des documents de travail.

³ Les dispositions réglementaires relatives à l'Observatoire figurent aux articles R. 144-1, R. 144-2 et R.142-22 à R. 142-27 du Code monétaire et financier.

ANNEXE C | LISTE NOMINATIVE DES MEMBRES DE L'OBSERVATOIRE

La composition de l'Observatoire a été définie par un arrêté du ministre de l'économie, des finances et de l'industrie du 20 avril 2006, complété par un arrêté du 22 juin 2006. Elle a été modifiée en 2007 par deux arrêtés en date du 27 juin et du 25 octobre 2007, ainsi qu'en 2009 par un arrêté en date du 29 juin 2009.

Liste des membres depuis le 29 juin 2009

Président

Christian NOYER
Gouverneur de la Banque de France

Représentants des assemblées

Jean-Pierre BRARD

Député

Nicole BRICQ

Sénatrice

Représentants du secrétaire général de l'Autorité de contrôle prudentiel

Jean-Luc MENDA

Direction de la surveillance générale du système bancaire

Philippe RICHARD

Secrétariat général

Représentants des administrations

Sur proposition du secrétariat général de la défense nationale :

- Le directeur central de la sécurité des systèmes d'information ou son représentant :
Patrick PAILLOUX

Sur proposition du ministre de l'économie, de l'industrie et de l'emploi :

- Le haut fonctionnaire de défense :
Emmanuel SARTORIUS

– Le directeur général du Trésor ou son représentant :

Henri JOHANET
Alexis ZAJDENWEBER
Marianne CARRUBBA

Sur proposition du ministre chargé de la consommation :

- Le directeur de la direction générale de la concurrence, de la consommation et de la répression des fraudes ou son représentant :
Jean-Pierre GERSKOUREZ
Serge DORE

Sur proposition du garde des sceaux, ministre de la justice :

- Le directeur des affaires criminelles et des grâces ou son représentant :
Alexandra VAILLANT
Cédric SAUNIER

Sur proposition du ministre de l'intérieur :

- Le chef de l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication ou son représentant :
Christian AGHROUM
Adeline CHAMPAGNAT

Sur proposition du ministre de la défense :

- Le directeur général de la gendarmerie nationale ou son représentant :
Éric FREYSSINET

Sur proposition du ministre délégué de l'industrie :

- Le directeur général des entreprises ou son représentant :
Mireille CAMPANA

Représentants des émetteurs de cartes de paiement

Yves BLAVET

Directeur des Instruments de Paiement – Société Générale

Jean-Marc BORNET

Administrateur – Groupement des Cartes Bancaires

Jean-François DUMAS

Vice Président – American Express France

Bernard DUTREUIL

Directeur – Fédération bancaire française

Bernard GOURAUD

Directeur des technologies – Banque Populaire – Caisse d'Epargne

François LANGLOIS

Directeur des Relations institutionnelles – BNP Paribas Personal Finance

Frédéric MAZURIER

Directeur administratif et financier – Société des Paiements Pass (S2P)

Gérard NEBOUY

Directeur Général – Visa Europe France

Emmanuel PETIT

Président Directeur Général – Mastercard France

Narinda VIGUIER

Directeur – Stratégie et pilotage interbancaire – Crédit Agricole SA

Représentants du collège « consommateurs » du Conseil national de la consommation

Régis CREPY

Confédération nationale – Associations familiales catholiques (CNAFC)

Valérie GERVAIS

Secrétaire générale – Association FO Consommateurs (AFOC)

Christian HUARD

Secrétaire général – Association de défense d'éducation et d'information du consommateur (ADEIC)

Jean-Pierre JANIS

Association Léo Lagrange pour la défense des consommateurs (ALLDC)

Représentants des organisations professionnelles de commerçants

Philippe JOGUET

Chef du service réglementation et développement durable – Fédération des entreprises du commerce et de la distribution (FCD)

Marc LOLIVIER

Délégué général – Fédération du e-commerce et de la vente à distance (Fevad)

Jean-Jacques MELI

Chambre de commerce et d'industrie du Val d'Oise

Jean-Marc MOSCONI

Délégué général – Mercatel

Philippe SOLIGNAC

Vice-président – Chambre de commerce et d'industrie de Paris/ACFCI

Personnalités qualifiées en raison de leurs compétences

Philippe CAMBRIEL

Executive Vice-President – Gemalto

David NACCACHE

Professeur – Ecole normale supérieure

Sophie NERBONNE

Directeur adjoint à la direction des affaires juridiques, internationales et de l'expertise – Commission nationale de l'informatique et des libertés (CNIL)

ANNEXE D | DOSSIER STATISTIQUE

Le dossier statistique qui suit a été réalisé à partir des données fournies à l'Observatoire de la sécurité des cartes de paiement par :

- les 136 membres du Groupement des Cartes Bancaires « CB » par l'intermédiaire de celui-ci, ainsi que de MasterCard et de Visa Europe France pour les données internationales ;
- dix émetteurs de cartes privatives : American Express, Banque Accord, BNP Paribas Personal Finance, Cofidis, Cofinoga, Diners Club, Finaref, Franfinance, S2P et Sofinco ;
- les émetteurs du porte-monnaie électronique Moneo.

L'Observatoire a également reçu des statistiques recueillies par la Fevad auprès d'un échantillon représentatif de ses membres.

Total des cartes en circulation en 2009 : 90,6 millions

- dont 62,4 millions de cartes de type « interbancaire » (« CB », MasterCard et Moneo) ;
- et 28,2 millions de cartes de type « privatif ».

Cartes mises en opposition en 2009 : environ 605 000

Les transactions nationales sont celles qui mettent en jeu un émetteur français et un commerçant accepteur français. Les transactions internationales sont de deux types : émetteur français / accepteur étranger et émetteur étranger / accepteur français.

Le marché des cartes de paiement en France

Cartes de type « interbancaire »	Émetteur français, Acquéreur français		Émetteur français, Acquéreur étranger		Émetteur étranger, Acquéreur français	
	Volume (millions)	Valeur (Md€)	Volume (millions)	Valeur (Md€)	Volume (millions)	Valeur (Md€)
Paiements de proximité et sur automate	6 118,98	271,57	130,92	9,41	149,19	12,14
Paiements à distance hors Internet	123,28	11,19	9,06	0,94	7,11	2,40
Paiements à distance sur Internet	245,97	19,08	66,56	3,48	12,84	1,63
Retraits	1 492,38	108,73	41,87	4,97	29,72	5,04
Total	7 980,61	410,56	248,42	18,80	198,85	21,21
Cartes de type « privatif »	Volume (millions)	Valeur (Md€)	Volume (millions)	Valeur (Md€)	Volume (millions)	Valeur (Md€)
Paiements de proximité et sur automate	229,20	20,76	8,78	1,60	13,09	2,40
Paiements à distance hors Internet	3,98	0,31	0,15	0,02	0,22	0,02
Paiements à distance sur Internet	5,75	0,63	0,32	0,04	0,47	0,06
Retraits	9,17	0,86	nd	nd	nd	nd
Total	248,10	22,55	9,24	1,66	13,78	2,49
Total général	8 228,72	433,11	257,67	20,46	212,63	23,70

Source : Observatoire de la sécurité des cartes de paiement

Répartition de la fraude selon le type de transaction, son origine et la zone géographique pour les cartes de type « interbancaire »

	Émetteur français, Acquéreur français		Émetteur français, Acquéreur étranger		Émetteur étranger, Acquéreur français	
	Volume (milliers)	Valeur (k€)	Volume (milliers)	Valeur (k€)	Volume (milliers)	Valeur (k€)
Paiements de proximité et sur automate	462,2	35 642,0	214,2	42 660,3	338,0	68 778,1
Cartes perdues ou volées	379,5	33 116,3	74,9	8 784,7	99,1	10 236,2
Cartes non parvenues	9,6	581,8	1,7	218,9	3,9	525,3
Cartes altérées ou contrefaites	37,1	1 937,4	124,4	31 039,8	75,0	25 947,3
Numéro de carte usurpé	0,0	6,6	6,3	1 832,0	78,3	16 192,4
Autres	0,0	0,0	6,9	748,8	81,8	15 849,8
Paiements à distance hors Internet	376,6	27 345,9	55,1	8 604,5	Nd	Nd
Cartes perdues ou volées	0,4	31,1	17,5	2 558,3	Nd	nd
Cartes non parvenues	0,0	1,1	0,1	15,8	nd	nd
Cartes altérées ou contrefaites	0,0	1,0	13,1	2 250,3	nd	nd
Numéro de carte usurpé	397,1	27 312,5	17,0	2 221,8	nd	nd
Autres	0,0	0,2	7,4	1 528,2	nd	nd
Paiements à distance sur Internet	365,9	51 576,1	464,6	50 594,0	nd	nd
Cartes perdues ou volées	0,6	109,3	141,7	14 342,8	nd	nd
Cartes non parvenues	0,0	0,1	0,4	44,8	nd	nd
Cartes altérées ou contrefaites	0,0	2,3	104,7	12 041,3	nd	nd
Numéro de carte usurpé	365,3	51 463,9	151,8	16 446,4	nd	nd
Autres	0,0	0,5	66,0	7 718,8	nd	nd
Retraits	85,5	19 838,3	103,2	16 467,2	9,1	2 754,5
Cartes perdues ou volées	82,2	19 367,1	11,5	1933,6	3,0	691,4
Cartes non parvenues	1,3	172,8	0,1	24,6	0,1	29,1
Cartes altérées ou contrefaites	2,0	298,3	88,8	14 069,3	5,8	2 002,1
Numéro de carte usurpé	0,0	0,0	0,2	24,8	0,1	14,7
Autres	0,0	0,0	2,5	414,9	0,1	17,2
Total	1 275,2	134 402,3	837,1	118 326,0	347,2	71 532,6

Source : Observatoire de la sécurité des cartes de paiement

Répartition de la fraude selon le type de transaction, son origine et la zone géographique pour les cartes de type « privatif »

	Émetteur français, Acquéreur français		Émetteur français, Acquéreur étranger		Émetteur étranger, Acquéreur français	
	Volume (milliers)	Valeur (k€)	Volume (milliers)	Valeur (k€)	Volume (milliers)	Valeur (k€)
Paiements de proximité et sur automate	13,96	5 376,17	8,56	2 023,30	3,30	1 013,51
Cartes perdues ou volées	4,87	925,38	1,17	192,97	0,27	54,72
Cartes non parvenues	3,47	608,37	0,35	139,63	0,05	17,57
Cartes altérées ou contrefaites	0,78	236,21	4,30	911,98	1,07	272,51
Numéro de carte usurpé	0,31	307,45	0,03	13,69	0,01	14,36
Autres	4,53	3 298,76	2,71	765,03	1,90	654,35
Paiements à distance hors Internet	7,30	2 987,62	6,54	1 089,87	6,52	3 585,02
Cartes perdues ou volées	1,85	703,22	2,12	112,56	0,84	384,43
Cartes non parvenues	0,73	209,74	0,05	13,18	0,37	146,35
Cartes altérées ou contrefaites	2,15	761,29	1,60	378,97	3,20	1 682,84
Numéro de carte usurpé	0,32	220,85	0,00	0,00	0,01	1,66
Autres	2,26	1 092,52	2,78	585,17	2,11	1 369,74
Paiements à distance sur Internet	0,83	218,12	0,91	197,98	4,90	686,67
Cartes perdues ou volées	0,10	25,25	0,01	1,31	0,22	48,01
Cartes non parvenues	0,01	5,06	0,01	2,10	0,04	4,00
Cartes altérées ou contrefaites	0,02	2,56	0,01	7,46	0,23	35,94
Numéro de carte usurpé	0,14	64,18	0,00	0,60	0,00	0,57
Autres	0,56	185,07	0,88	168,50	4,40	598,14
Retraits	3,19	935,99	nd	Nd	nd	nd
Cartes perdues ou volées	2,65	748,97	nd	nd	nd	nd
Cartes non parvenues	0,29	121,25	nd	nd	nd	nd
Cartes altérées ou contrefaites	0,00	0,00	nd	nd	nd	nd
Numéro de carte usurpé	0,00	0,00	nd	nd	nd	nd
Autres	0,24	65,77	nd	nd	nd	nd
Total	25,28	9 581,90	16,01	3 295,15	14,72	5 285,20

Source : Observatoire de la sécurité des cartes de paiement

ANNEXE E | DÉFINITION ET TYPOLOGIE DE LA FRAUDE RELATIVE AUX CARTES DE PAIEMENT

Définition de la fraude

A des fins de recensement statistique, l'Observatoire estime qu'il convient de considérer comme constitutif de fraude :

Toute utilisation illégitime d'une carte de paiement ou des données qui lui sont attachées, ainsi que tout acte concourant à la préparation ou à la réalisation d'une telle utilisation :

1. ayant pour conséquence un préjudice pour le banquier teneur de compte qu'il s'agisse du banquier du porteur de la carte ou de celui de l'accepteur (commerçant, administration... pour son propre compte ou au sein d'un système de paiement¹), le porteur, l'accepteur, l'émetteur, un assureur, un tiers de confiance ou tout intervenant dans la chaîne de conception, de fabrication, de transport, de distribution de données physiques ou logiques, dont la responsabilité civile, commerciale ou pénale pourrait être engagée ;
2. quels que soient :
 - les moyens employés pour récupérer, sans motif légitime, les données ou le support de la carte (vol, détournement du support de la carte, des données physiques ou logiques, des données de personnalisation et/ou récupération du code secret, et/ou du cryptogramme, piratage de la piste magnétique et/ou de la puce...);
 - les modalités d'utilisation de la carte ou des données qui lui sont attachées (paiement ou retrait, en paiement de proximité ou à distance, par utilisation physique de la carte ou du numéro de carte, sur automate...);
 - la zone géographique d'émission ou d'utilisation de la carte ou des données qui lui sont attachées :
 - émetteur français et carte utilisée en France,
 - émetteur étranger et carte utilisée en France,
 - émetteur français et carte utilisée à l'étranger ;
 - le type de carte de paiement², y compris les porte-monnaie électroniques.
3. que le fraudeur soit un tiers, le banquier teneur de compte, le porteur de la carte lui-même (dans le cas par exemple d'une utilisation après déclaration de vol ou de perte, ou d'une dénonciation abusive de transactions), l'accepteur, l'émetteur, un assureur, un tiers de confiance...

¹ Dans le cas d'Internet, l'accepteur peut être différent du fournisseur de service, ou d'un tiers de confiance (paiements, dons effectués par des internautes en soutien d'un site, d'une idéologie...).

² Tel que défini à l'article L. 132-1 du Code monétaire et financier dans sa version antérieure au 1^{er} novembre 2009.

Typologie de la fraude

L'Observatoire a par ailleurs défini une typologie de la fraude qui distingue les éléments suivants.

Les origines de fraude :

- *carte perdue ou volée* : le fraudeur utilise une carte de paiement obtenue à l'insu de son titulaire légitime, suite à une perte ou à un vol ;
- *carte non parvenue* : la carte a été interceptée lors de son envoi à son titulaire légitime par l'émetteur. Ce type d'origine se rapproche de la perte ou du vol. Cependant, il s'en distingue, dans la mesure où le porteur peut moins facilement constater qu'un fraudeur est en possession d'une carte lui appartenant et où il met en jeu des vulnérabilités spécifiques aux procédures d'envoi des cartes ;
- *carte falsifiée ou contrefaite* : une carte de paiement authentique est falsifiée par modification des données magnétiques, d'embossage ou de programmation. La contrefaçon d'une carte suppose la création d'un support donnant l'illusion d'être une carte de paiement authentique et/ou susceptible de tromper un automate ou une personne quant à sa qualité substantielle. Pour les paiements effectués sur automate de paiement, une telle carte, fabriquée par le fraudeur, supporte les données nécessaires à tromper le système. En commerce de proximité, une carte contrefaite est une carte fabriquée par un fraudeur, qui présente certaines sécurités (dont l'aspect visuel) d'une carte authentique, supporte les données d'une carte authentique et est destinée à tromper la vigilance d'un accepteur ;
- *numéro de carte usurpé* : le numéro de carte d'un porteur est relevé à son insu ou créé par « moulinage » (voir le paragraphe sur les techniques de fraude ci-dessous) et utilisé en vente à distance ;
- *numéro de carte non affecté* : utilisation d'un PAN³ cohérent mais non attribué à un porteur, puis généralement utilisé en vente à distance ;
- *fractionnement du paiement* : action qui consiste à scinder le paiement en vue de passer en dessous des plafonds fixés par l'émetteur.

Les techniques de fraude :

- *skimming* : technique qui consiste en la copie, dans un commerce de proximité ou dans des distributeurs automatiques, des pistes magnétiques d'une carte de paiement à l'aide d'un lecteur à mémoire appelé « skimmer ». Éventuellement, le code confidentiel est également capturé de visu, à l'aide d'une caméra ou encore par détournement du clavier numérique. Ces données seront inscrites ultérieurement sur les pistes magnétiques d'une carte contrefaite ;
- *ouverture frauduleuse de compte* : ouverture d'un compte de référence en fournissant de fausses données personnelles ;
- *usurpation d'identité* : actes frauduleux liés à un paiement par carte et supposant l'utilisation de l'identité d'une autre personne ;
- *répudiation abusive* : contestation par le porteur, de mauvaise foi, d'un ordre de paiement valide dont il est l'initiateur ;
- *piratage d'automates de paiement ou de retrait* : techniques qui consistent à placer des dispositifs de duplication de cartes sur des automates de paiement ou des distributeurs automatiques de billets ;

³ Personal Account Number

- *piratage de systèmes automatisés de données, de serveurs ou de réseaux* : intrusion frauduleuse sur de tels systèmes ;
- *moulinage* : technique de fraude consistant à utiliser les règles, propres à un émetteur, de création de numéros de cartes pour générer de tels numéros et effectuer des paiements.

Les types de paiement :

- *paiement de proximité*, réalisé au point de vente ou sur automate ;
- *paiement à distance* réalisé sur Internet, par courrier, par fax/téléphone, ou par tout autre moyen ;
- *retrait* (retrait DAB ou autre type de retrait).

La répartition du préjudice entre :

- la banque du commerçant, acquéreur de la transaction ;
- la banque du porteur, émettrice de la carte ;
- le commerçant ;
- le porteur ;
- les éventuelles assurances ;
- et les autres types d'acteurs.

La zone géographique d'émission ou d'utilisation de la carte ou des données qui lui sont attachées :

- l'émetteur et l'acquéreur sont, tous deux, établis en France. On dira également, dans ce cas, que la transaction est nationale ;
- l'émetteur est établi en France et l'acquéreur est établi à l'étranger ;
- l'émetteur est établi à l'étranger et l'acquéreur est établi en France.

Directeur de la publication

Robert Ophèle

Directeur général des opérations
Banque de France

Rédacteur en chef

Yvon Lucas

Directeur des systèmes de paiement
et infrastructures de marché
Banque de France

Imprimerie Banque de France

Ateliers SIMA

Document achevé de rédiger le 1^{er} juillet 2010

Dépôt légal 3^{ème} trimestre 2010

ISSN 1768-2991

